

## PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

## NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner  
US Department of Commerce  
United States Patent and Trademark  
Office, PCT  
2011 South Clark Place Room  
CP2/5C24  
Arlington, VA 22202  
ETATS-UNIS D'AMERIQUE  
in its capacity as elected Office

Date of mailing (day/month/year) 19 February 2001 (19.02.01)	
International application No. PCT/DE00/01901	Applicant's or agent's file reference 99PH 1131 DEP
International filing date (day/month/year) 16 June 2000 (16.06.00)	Priority date (day/month/year) 17 June 1999 (17.06.99)
Applicant MEYER-GRÄFE, Karsten et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:09 January 2001 (09.01.01)☐ in a notice effecting later election filed with the International Bureau on:2. The election ☒ was☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Kiwa Mpay Telephone No.: (41-22) 338.83.38
---	---

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT IM GEBIET DES  
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
28. Dezember 2000 (28.12.2000)

PCT

(10) Internationale Veröffentlichungsnummer  
WO 00/79352 A2

(51) Internationale Patentklassifikation: G05B 19/042

Karsten [DE/DE]: Lupinenweg 8, D-33161 Hövelhof  
(DE). KREß, Wolfram [DE/DE]: Auf dem Gerotzen 16,  
D-53721 Siegburg (DE).

(21) Internationales Aktenzeichen: PCT/DE00/01901

(22) Internationales Anmeldedatum:  
16. Juni 2000 (16.06.2000)

(74) Anwalt: HERDEN, Andreas; Blumbach, Kramer & Part-  
ner GbR, Alexandrasstrasse 5, D-65187 Wiesbaden (DE).

(25) Einreichungssprache: Deutsch

(81) Bestimmungsstaaten (national): JP, US.

(26) Veröffentlichungssprache: Deutsch

(84) Bestimmungsstaaten (regional): europäisches Patent (AT,  
BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,  
NL, PT, SE).

(30) Angaben zur Priorität:  
199 27 635.8 17. Juni 1999 (17.06.1999) DE

Veröffentlicht:

— Ohne internationalen Recherchenbericht und erneut zu  
veröffentlichen nach Erhalt des Berichts.

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von  
US): PHOENIX CONTACT GMBH & CO. [DE/DE];  
Flachmarktstrasse 8-28, D-32825 Blomberg (DE).

Zur Erklärung der Zweibuchstaben-Codes, und der anderen  
Abkürzungen wird auf die Erklärungen ("Guidance Notes on  
Codes and Abbreviations") am Anfang jeder regulären Ausgabe  
der PCT-Gazette verwiesen.

(72) Erfinder; und

(73) Erfinder/Anmelder (nur für US): MEYER-GRÄFE,

(54) Title: SECURITY-RELATED BUS AUTOMATION SYSTEM

(54) Bezeichnung: SICHERHEITSBEZOGENES AUTOMATISIERUNGSBUSSYSTEM

(57) Abstract: The invention relates to a security-related automation system and a method for operating said system. In order to produce a security-related bus automation system which involves a minimum amount of hardware redundancy and which can be adapted to requirements in a flexible manner, the automation system comprises at least one security analyzer which is connected to the bus by means of an interface and which monitors the data flow via said bus, whereby the analyzer is configured in such a way that it can execute security-related functions. The automation system is characterized in that a standard control device controls at least one security-related output and the security analyzer is configured in such a way that it can monitor and/or process security-related data in the bus data flow.

(57) Zusammenfassung: Die Erfindung betrifft ein sicherheitsbezogenes Automatisierungssystem und ein Verfahren zum Betrieb eines derartigen Systems. Um ein sicherheitsbezogenes Automatisierungsbussystem bereitzustellen, welches mit einer geringen Hardware-Redundanz auskommt und flexibel an die jeweiligen Anforderungen angepaßt werden kann, umfaßt das Automatisierungssystem zumindest einen Sicherheitsanalysator, der mittels einer Schnittstelle an den Bus angeschlossen ist und den Datenfluß über den Bus mitbört, wobei der Analysator zum Ausführen von sicherheitsbezogenen Funktionen eingerichtet ist. Das Automatisierungssystem zeichnet sich dadurch aus, daß die Standardsteuereinrichtung zumindest einen sicherheitsbezogenen Ausgang ansteuert und der Sicherheitsanalysator zur Überprüfung und/oder zum Verarbeiten von sicherheitsbezogenen Daten im Busdatenstrom ausgebildet ist.

WO 00/79352 A2

Phoenix Contact GmbH &amp; Co

Sicherheitsbezogenes Automatisierungsbussystem

- 5 Die Erfindung betrifft ein sicherheitsbezogenes  
Automatisierungsbussystem nach dem Oberbegriff des Anspruchs  
1 und ein Verfahren zum Betrieb eines derartigen Systems.
- Steuer- und Datenübertragungsanlagen haben aufgrund des damit  
10 möglichen hohen Automatisierungsgrades eine herausragende  
Stellung nicht nur in der industriellen Fertigung erlangt.  
Derartige Automatisierungssysteme weisen im allgemeinen  
zumindest Abschnitte oder Komponenten auf, an welche erhöhte  
Anforderungen im Hinblick auf die Sicherheit zu stellen sind.  
15 Beispielsweise muß sichergestellt sein, daß bestimmte  
Maschinen innerhalb vorgegebener Betriebsparameter betrieben  
werden oder es muß verhindert werden, daß eine Maschine  
läuft, obwohl sich eine Person in deren Arbeitsbereich  
aufhält. In dieser Hinsicht darf beispielsweise eine  
20 Drehmaschine nicht eine vorgegebene Drehzahl überschreiten  
oder sich nicht beim Betrieb eines Roboters eine Person im  
Aktionsradius des Roboters aufhalten. Weiterhin muß beim  
Betrieb eines Automatisierungssystems sichergestellt sein,  
daß bei einem Ausfall einer Komponente des Systems die Anlage  
25 nicht in einen undefinierten und damit nicht vorhersagbaren  
Zustand gerät.

Ein Ansatz für diese Problematik nach dem Stand der Technik  
besteht darin, insbesondere die sicherheitsrelevanten

Komponenten des Systems mehrkanalig, d.h. redundant aufzubauen. Beispielsweise kann in einem Automatisierungsbussystem vorgesehen sein, Sicherheitsbuskomponenten, d.h. z.B. Busteilnehmer, die einer sicherheitsrelevanten Maschine zugeordnet sind, doppelt auszuführen. Gleichzeitig kann auch die zentrale Steuerung und der Bus mehrkanalig aufgebaut sein oder gar eine von der Prozeßsteuerung getrennte spezielle und unter Umständen redundant aufgebaute Sicherheitssteuerung zur Steuerung der sicherheitsrelevanten Komponenten vorgesehen sein. Diese Sicherheitssteuerung führt im wesentlichen die Verknüpfungen der sicherheitsbezogenen Eingangsinformationen durch und übermittelt daraufhin, beispielsweise über einen Automatisierungsbuss, sicherheitsbezogene Verknüpfungsdaten an Ausgangskomponenten. Die Ausgangskomponenten ihrerseits bearbeiten die empfangenen Sicherheitsmaßnahmen und geben nach positiver Prüfung diese an die Peripherie aus. Darüber hinaus schalten sie ihre Ausgänge in einen sicheren Zustand, wenn sie einen Fehler feststellen oder innerhalb einer vorgegebenen Zeitdauer keine gültigen Daten mehr empfangen haben.

Der Einsatz von zwei Steuerungen im System, d.h. eine Prozeßsteuerung sowie der beschriebenen Sicherheitssteuerung hat jedoch einige Nachteile zur Folge. Gerade aufgrund steigender Anforderungen an die Reaktionszeit von Automatisierungssystemen muß ein derartiges System häufig auf Sicherheitsinseln aufgeteilt werden. Weiterhin treten insbesondere bei mehrkanaligen Steuerungssystemen Synchronisationsprobleme auf, welche trotz prinzipiell intakter Anlage zu Ausfällen oder gar Zerstörungen von Maschinenteilen führen können. Weiterhin zieht der mehrkanalige Aufbau durch den vergrößerten Hardware-Aufwand

eine Erhöhung der System- als auch der Wartungskosten nach sich.

5 Aus DE 198 15 150 A1 ist ein System bekannt, welches eine an den Bus angeschlossene Auswerteeinheit umfaßt, die fortlaufend die über das Bussystem übertragenen Signale abhört und nur bei fehlerfreier Identifizierung von über das Bussystem übertragenen Kodierungen ein Arbeitsgerät in Betrieb setzt. Hierzu werden die durch den Busteilnehmer an  
10 den Master gesendeten Eingangsdaten ausgewertet und im Ansprechen auf die Auswertung das Arbeitsgerät eingeschaltet oder ausgeschaltet belassen.

15 Ein derartiger Ansatz ist im Vergleich zur erstbeschriebenen Anlage nicht so kostenintensiv, er ist jedoch sehr unflexibel im Hinblick auf eine Erweiterung des Systems oder eine Anpassung der Anlage an andere Buskomponenten. Weiterhin ist die Auswerteeinheit allein für das Auslösen einer sicherheitsgerichteten Funktion zuständig, so daß zur  
20 Einhaltung hoher Sicherheitsanforderungen die Auswerteeinheit zwingend redundant ausgeführt werden muß.

Aufgabe der Erfindung ist es somit, ein sicherheitsbezogenes Automatisierungsbussystem bereitzustellen, welches möglichst  
25 mit einer geringen Hardware-Redundanz auskommt und flexibel an die jeweiligen Anforderungen angepaßt werden kann.

Die Erfindung löst dieses Problem mit einem Automatisierungsbussystem mit den Merkmalen des Anspruchs 1  
30 sowie ein Verfahren zum Betrieb einer derartigen Steuer- und Datenverarbeitungsanlage nach Anspruch 14. Weiterbildungen der Erfindung sind in den Unteransprüchen angegeben.

Erfindungsgemäß umfaßt das Automatisierungssystem ein Bussystem, daran angeschlossene Sensor- und Aktor-Busteilnehmer und eine Standardsteuerungseinrichtung, welche die Prozeßsteuerung mit der Verarbeitung von prozeßgebundenen E/A-Daten und eine sicherheitsbezogene Steuerung mit der Verarbeitung von sicherheitsbezogenen Daten, d.h. der Steuerung von sicherheitsbezogenen Ein- und Ausgängen, durchführt. Weiterhin ist ein sogenannter Sicherheitsanalysator umfaßt, der mittels einer entsprechenden Schnittstelle an den Bus angeschlossen ist und den Datenfluß über den Bus mithört, wobei der Analysator zum Ausführen von sicherheitsbezogenen Funktionen eingerichtet ist. Dies betrifft beispielsweise die Ansteuerung eines Schützes zum Abschalten der Versorgungsspannung von Systemkomponenten oder die Ermittlung von Qualitätsdaten. Derartige Qualitätsdaten können allgemeine Systemparameter, z.B. Daten über das Auftreten von Fehlern in Systemkomponenten oder Busübertragungsfehlern umfassen. Das Automatisierungssystem zeichnet sich dadurch aus, daß die Standardsteuereinrichtung zumindest einen sicherheitsbezogenen Ausgang über den Bus ansteuert, sie kann jedoch auch selbst einen derartigen sicherheitsbezogenen Ausgang aufweisen. Erfindungsgemäß bezeichnet ein sicherheitsbezogener Ausgang eine Senke einer Sicherheitsinformation, die in Abhängigkeit der Information sicherheitsgerichtete Abläufe startet, beispielsweise eine Maschine herunterfährt oder gar durch Unterbrechen des Versorgungsstromes eine Maschine abschaltet. Der Sicherheitsanalysator ist im erfindungsgemäßen Automatisierungssystem zur Überprüfung und/oder zum Verarbeiten von sicherheitsbezogenen Daten, insbesondere sicherheitsbezogenen Verknüpfungsdaten im Busdatenstrom ausgebildet. Dabei sind sicherheitsbezogene Verknüpfungsdaten

beispielsweise Daten, welche die sicherheitsbezogene Steuerung nach der Verarbeitung von sicherheitsbezogenen Daten an sicherheitsbezogene Ausgänge sendet.

- 5 Damit wird ein System bereitgestellt, welches extrem flexibel auf die jeweiligen Anforderungen an das Automatisierungssystem eingestellt werden kann. Beispielsweise kann jeder Sicherheitsbuskomponente ein derartiger Sicherheitsanalysator zugeordnet oder auch ein
- 10 Sicherheitsanalysator in die Sicherheitskomponente, beispielsweise einen Sicherheitsbusteilnehmer selbst integriert werden, es ist jedoch auch möglich, daß ein einzelner Sicherheitsanalysator die Verarbeitung sicherheitsbezogener Daten oder die Überprüfung der
- 15 sicherheitsbezogenen Verknüpfungsdaten im Busdatenstrom für mehrere Sicherheitsbuskomponenten oder gar alle Sicherheitsbuskomponenten des Systems vornimmt.

- Das Prinzip der Erfindung beruht auf der Erkenntnis des
- 20 Erfinders, daß die in heutigen Automatisierungsanlagen eingesetzte Elektronik selbst nur selten ausfällt. Die Integration der aktuellen digitalen Sicherheitstechnik in die Automatisierungstechnik in Form von Sicherheitssteuerungen oder Sicherheitsbussystemen nach dem Stand der Technik hat
- 25 häufig den Nachteil einer abnehmenden Verfügbarkeit des Systems. Um diese Ausfallzeiten zu reduzieren, kommen deshalb neben den genannten Sicherheitskomponenten auch Verfügbarkeitsstrukturen zum Einsatz, die ihrerseits aber zu einer nicht unerheblichen Zunahme der Kosten durch den
- 30 erhöhten Hardware-Aufwand führen.

Die Erfindung setzt deshalb auf der Zuverlässigkeit heutiger Automatisierungssysteme auf und integriert eine reine

Notfall-Elektronik bzw. -Software, die erst dann aktiv in den Betrieb der Anlage eingreift, wenn die Standardtechnik fehlerhaft arbeitet. Die Standardsteuerungseinrichtung verarbeitet deshalb auch sicherheitsbezogene Daten, d.h. sie steuert sicherheitsrelevante Ein- und Ausgänge. Insbesondere die erzeugten sicherheitsbezogenen Verknüpfungsdaten im Busdatenstrom werden jedoch vom Sicherheitsanalysator abgehört und überprüft. Dies hat für den Anwender den Vorteil, daß eine strikte Trennung der Sicherheitstechnik und der Standardtechnik bei der Programmierung nicht mehr unbedingt notwendig ist. Das erfindungsgemäße Automatisierungssystem ist auf alle Systeme mit einem Bus, insbesondere auf Bussysteme mit Master-Slave-Buszugriffsverfahren anwendbar. Unabhängig von der Anordnung des Sicherheitsanalysators im Fernbus-Abschnitt kann dieser bei einem beispielhaften seriellen Bussystem nach EN 50 254 alle IN-Daten auf dem Bus lesen, der Umfang der mithörbaren OUT-Daten hängt jedoch von der Anordnung des Sicherheitsanalysators im System ab. Die Bezeichnung Busdatenstrom bezeichnet dabei erfindungsgemäß alle über dem Bus übermittelte Informationen, insbesondere auch die in einem Summenrahmen über den Bus transportierten Daten.

Um den einschlägigen Sicherheitsanforderungen zu genügen, kann der Sicherheitsanalysator im Ansprechen auf die Überprüfung und/oder die Verarbeitung von sicherheitsbezogenen Daten, insbesondere von Verknüpfungsdaten im Busdatenstrom, die notwendigen sicherheitsbezogenen Funktionen auslösen. Hierbei kann der Sicherheitsanalysator sowohl auf OUT-Daten, d.h. Verknüpfungsdaten der Standardsteuereinrichtung reagieren als auch auf IN-Daten, d.h. Informationen im Busdatenstrom, welche von einzelnen E/A-Busteilnehmern an die



Standardsteuereinrichtung gesendet wurden.

- Um einen Fehler in sicherheitsbezogenen Verknüpfungsdaten, welche über den Bus transportiert werden, zu erkennen, kann
- 5 der Sicherheitsanalysator eine frei programmierbare Logikeinrichtung aufweisen, in welcher die abgehörten Daten, insbesondere die abgehörten sicherheitsbezogenen Daten verarbeitet werden. Auf diese Weise kann der Sicherheitsanalysator durch das Nachbilden der
- 10 sicherheitsbezogenen Verknüpfungen der Standardsteuerung deren als OUT-Daten über den Bus gesendeten Verknüpfungsdaten überprüfen und im Ansprechen auf die Überprüfung oder den Vergleich notwendige sicherheitsbezogene Funktionen ausführen. Um die Anlage beispielsweise in einen sicheren
- 15 Zustand zu bringen, kann der Sicherheitsanalysator einen Ausgang umfassen, über welchen eine Baugruppe, insbesondere ein Busteilnehmer des Automatisierungsbussystems ein- oder ausschaltbar ist. Die Abschaltung kann durch Trennen von der Spannungsversorgung realisiert werden. Um zusammenhängende
- 20 bzw. voneinander abhängende Busteilnehmer in Gesamtheit in einen sicheren Zustand zu bringen, kann der Sicherheitsanalysator zur Abschaltung eines Busstichs, einer mehrere, einander zugeordnete Busteilnehmer umfassende Sicherheitsinsel oder zum Abschalten von Komponenten nach
- 25 einer im Analysator abgelegten Verriegelungslogik eingerichtet sein. Es ist jedoch auch möglich, daß über den sicherheitsbezogenen Ausgang des Sicherheitsanalysators die Gesamtanlage von der Spannungsversorgung abgetrennt wird.
- 30 Der Sicherheitsanalysator kann sicherheitsbezogene Informationen neben dem Abhören des Busses weiterhin über einen direkten Eingang erfassen, mittels welchem der Sicherheitsanalysator mit einer sicherheitsbezogenen

Einrichtung des Automatisierungsbussystems verbunden ist.  
Diese Einrichtung kann dabei, muß aber nicht an den Bus  
angeschlossen sein. Beispielsweise umfaßt die so zugängliche  
sicherheitsbezogene Information die Momentandrehzahl der  
5 schon erwähnten Drehmaschine, wobei der Analysator im Falle  
des Überschreitens einer vorbestimmten Grenzdrehzahl die  
Maschine mittels ihres Ausgangs abschaltet.

Um eine Trennung der sicherheitsbezogenen Informationen und  
10 der Prozeßdaten im System und insbesondere in der Steuerung  
durchzuführen, kann das Bussystem über eine Anschaltbaugruppe  
mit einem Host verbunden sein, wobei die prozeßbezogene  
Steuerung der Standardsteuereinrichtung im Host und die  
sicherheitsbezogene Steuerung der Standardsteuereinrichtung  
15 in der Anschaltbaugruppe angeordnet ist. Vorteilhafterweise  
läßt sich die sicherheitsbezogene Steuerung beispielsweise in  
Form von Software-Funktionsbausteinen, welche die notwendigen  
Verknüpfungen der sicherheitsrelevanten E/A-Informationen  
vornehmen, realisieren.

20 Die sicherheitsbezogene Steuerung kann somit in gleicher  
Weise implementiert werden wie die Prozeßsteuerung. Bei der  
Codierung der sicherheitsbezogenen Verknüpfungen ist der  
Programmierer ebenso wie bei der Prozeßsteuerung von der  
verwendeten Programmiersprache unabhängig.

25 Die Verknüpfungen auf dem Sicherheitsanalysator haben in etwa  
denselben Umfang wie die Verknüpfungen auf dem Host  
beziehungsweise auf der Anschaltbaugruppe und können entweder  
in derselben oder aber in einer anderen Programmiersprache  
30 erstellt werden. Der Sicherheitsanalysator führt zusätzlich  
einen Vergleich der Verknüpfungen zwischen den Ergebnissen  
des Host-Systems beziehungsweise der Anschaltbaugruppe und  
seinen eigenen durch und startet beispielsweise beim

Auftreten von Ungleichheit sicherheitsgerichtete Funktionen.

Das Abnahmeverfahren eines solchen Systems kann erheblich einfacher erfolgen, als es bei den Systemen nach dem Stand der Technik der Fall ist. Die Anlage kann mit allen Sicherheitsverriegelungen in Betrieb genommen werden, ohne die Sicherheitstechnik aktiv geschaltet zu haben. Die notwendigen Verknüpfungen befinden sich dabei im Host-System oder in der Anschaltbaugruppe. Die Funktionsfähigkeit der Anlage kann zunächst im Black-Box-Test untersucht werden. In einem zweiten Schritt wird dann die Sicherheitstechnik in Form der beziehungsweise des Sicherheitsanalysators(en) zugeschaltet. Da dort nur die Sicherheitsverknüpfungen, nicht aber die Prozeßdatenverknüpfungen vorhanden sind, läßt sich nun der White-Box-Test schnell und übersichtlich durchführen, wodurch sich die Abnahmezeiten erheblich reduzieren lassen. Da die sicherheitsbezogenen Verknüpfungsalgorithmen auch auf dem Host-System beziehungsweise der Anschaltbaugruppe ablaufen, ist ein Vergleich mit denen des Analysators schnell möglich.

Wird der Bus als serieller Ringbus, beispielsweise als Bus gemäß EN 50254 ausgebildet, und ist ein Sicherheitsanalysator im Top-Level-Fernbus-Abschnitt des Automatisierungssystems angeordnet, so hat dieser Zugriff auf alle IN-Daten des Systems, da in dem bezeichneten System die Daten in einer hin- und in einer rückführenden Übertragungsleitung durch jeden Busteilnehmer geführt werden. Damit ist der Analysator in der Lage, ein auf die IN-Daten und die ihm zugänglichen Out-Daten beschränktes Prozeßabbild aufzubauen.

Bei Bussystemen mit Linientopologie kann der Sicherheitsanalysator in der Regel an jedem Ort im Bussystem

alle Information mitlesen und damit ein vollständiges Prozeßabbild anlegen.

5 In einer vorteilhaften Ausführungsform der Erfindung ist der Sicherheitsanalysator in einem seriellen Ringbussystem direkt nach dem Host oder der Anschaltbaugruppe angeordnet, so daß dieser ein vollständiges Prozeßabbild aufbauen kann. Somit ist der Sicherheitsanalysator in der Lage jederzeit und in vollem Umfang sicherheitsgerichtete Daten, insbesondere  
10 sicherheitsgerichtete Verknüpfungsdaten auf ihre Richtigkeit zu überprüfen beziehungsweise zu verarbeiten, da in diesem Fall der Analysator Zugriff auf alle In- und Out-Daten, d.h. alle Eingangs- und Ausgangsdaten besitzt.

15 Ist der Sicherheitsanalysator in der Anschaltbaugruppe des beschriebenen seriellen Ringbussystems angeordnet, so kann die Funktion des Sicherheitsanalysators mittels einer Softwarekomponente in der Anschaltbaugruppe ausgeführt sein. Vorteilhafterweise weist die Anschaltbaugruppe hierbei einen  
20 sicherheitsbezogenen Ausgang auf, um entsprechende sicherheitsgerichtete Funktionen, beispielsweise das Abschalten einer Versorgungsspannung mittels eines Schützes auszuführen.

25 Das Ausführen derartiger sicherheitsgerichteter Funktionen kann jedoch in einer besonderen vorteilhaften Ausführungsform der Erfindung durch direkte Datenmanipulation des Busdatenstroms durch den Sicherheitsanalysator realisiert werden. Das Manipulieren umfaßt das Umschreiben, das  
30 Ergänzen, das Einfügen sowie das Substituieren sowohl von OUT-Daten als auch von IN-Daten des Busdatenstroms. Bei Kenntnis des Prozeßabbildes kann somit der Sicherheitsanalysator in weitreichender Form auf den Betrieb

des erfindungsgemäßen Automatisierungssystems Einfluß nehmen und damit sicherstellen, daß die Anlage zu jedem Zeitpunkt in definierten Zuständen gehalten werden kann. Das Prinzip der Datenmanipulation kann weiterhin auch dazu benutzt werden, um  
5 einen in einem im Busstich angeordneten Sicherheitsanalysator im allgemeinen nicht zugängliche Busdatenstromanteile verfügbar zu machen, indem ein im Fernbus angeordneter Sicherheitsanalysator die betreffenden Daten in Daten wandelt, welche in den betreffenden Busstich transportiert  
10 werden. Auf diese Weise ist eine direkte Datenverbindung zwischen Sicherheitsanalysatoren realisiert.

Die Datenmanipulation durch einen Sicherheitsanalysator kann in einem nach dem Master-Slave-Prinzip arbeitenden Bussystem  
15 auch verwendet werden, um Daten zwischen zumindest zwei Slaves, insbesondere zwischen einzelnen Busteilnehmern, mittels einer Punkt-zu-Punkt-Verbindung über wenigstens einen Sicherheitsanalysator zu übertragen, wobei der Sicherheitsanalysator Daten im Busdatenstrom umkopiert. Der  
20 Master ist bei dieser Daten-Verbindung je nach Lage der beiden Slaves im Bussystem unter Umständen nicht eingebunden, so daß der Datentransport völlig unabhängig vom Busmaster realisiert wird. Eine derartige Datenverbindung zwischen zwei Slaves ist im übrigen auch durch die Ausführung einer  
25 Kopierfunktion durch den Busmaster möglich. Während bei einem Sicherheitsanalysator als Mittler, wie vorstehend beschrieben, zumindest in bestimmten Fällen der Busmaster nicht in den Datentransport eingebunden ist, ist der Busmaster für die zweite Form einer Punkt-zu-Punkt-Verbindung  
30 zwischen zwei Slaves zwingend notwendig.

Das Austauschen von Daten zwischen zumindest zwei Slaves, beispielsweise zwischen einzelnen Busteilnehmern, mittels

einer Punkt-zu-Punkt-Verbindung kann weiterhin auch durch die Einbindung des Masters oder der Steuerung in die Übertragung realisiert werden, wobei in diesem Fall der Master bzw. die Steuerung die Daten im Busdatenstrom umkopiert.

5

Zur Erhöhung der Datensicherheit können die sicherheitsbezogenen Daten in einem Sicherheitsprotokoll über den Bus übertragen werden. Beispielsweise kann das Sicherheitsprotokoll zusätzlich zu dem Sicherheitsdatum das  
10 negierte Sicherheitsdatum, eine laufende Nummer, eine Adresse und/oder eine Datensicherungsinformation (CRC) umfassen.

Die Flexibilität des Systems zeigt sich insbesondere in einer weiteren vorteilhaften Ausführungsform der Erfindung, bei  
15 welcher das erfindungsgemäße Automatisierungssystem mehrere Sicherheitsanalysatoren umfaßt, wobei in einem Sicherheitsanalysator ablaufende sicherheitsbezogene Verknüpfungen redundant in wenigstens einem weiteren Sicherheitsanalysator durchgeführt werden und durch beide  
20 Sicherheitsanalysatoren zumindest teilweise die gleichen Sicherheitsfunktionen ausgeführt und ausgelöst werden. Dabei können die betreffenden Sicherheitsanalysatoren zusätzlich zu den redundanten, d.h. auf beiden Analysatoren ablaufenden Verknüpfungen auch unterschiedliche sicherheitsbezogenen  
25 Verknüpfungen ausführen.

Die Erfindung wird im folgenden durch das Beschreiben einiger Ausführungsformen unter Zugrundelegen der Zeichnungen erläutert, wobei

30 Fig. 1 in einer Prinzipdarstellung eine erste Ausführungsform des erfindungsgemäßen Automatisierungssystems mit zwei Sicherheitsanalysatoren im Fernbus-Abschnitt zeigt,

- Fig. 2 in einer Prinzipskizze eine weitere Ausführungsform der Erfindung darstellt, wobei ein Sicherheitsanalysator direkt hinter der Anschaltbaugruppe angeordnet ist,
- 5 Fig. 3 das erfindungsgemäße Automatisierungssystem in einer Prinzipskizze mit einem in die Anschaltbaugruppe integrierten Sicherheitsanalysator sowie einem zweiten Sicherheitsanalysator am Kopf eines Busstichs zeigt,
- 10 Fig. 4 ein erfindungsgemäßes Automatisierungssystem mit zwei Sicherheitsanalysatoren darstellt, wobei deren Ausgänge miteinander verbunden sind,
- Fig. 5 in einer prinzipiellen Blockbilddarstellung einen Sicherheitsanalysator mit verschiedenen Ein- und Ausgängen zeigt und
- 15 Fig. 6a und 6b in einer Prinzipdarstellung die Datenmanipulation des Busdatenstroms durch den Sicherheitsanalysator zeigt.
- 20
- In Fig. 1 ist in einer Prinzipdarstellung das erfindungsgemäße Automatisierungssystem 1, d.h. eine Steuer- und Datenübertragungsanlage gemäß der Erfindung dargestellt. Es umfaßt einen Bus 2, an welchen E/A-Busteilnehmer mit zugeordneten Sensoren und Aktoren angeschlossen sind. Eine
- 25 Standardsteuerungseinrichtung 4 führt über den Bus die Prozeßsteuerung mit der Verarbeitung von prozeßgebundenen E/A-Daten durch. Hierzu empfängt die Steuerung 4 Daten von den einzelnen Busteilnehmern 31 - 38, die wiederum selbst von der Standardsteuerungseinrichtung Daten empfangen. Weiterhin
- 30 ist die Standardsteuerungseinrichtung mit der Verarbeitung von sicherheitsbezogenen Daten befaßt. In diesem Sinne übernimmt die Standardsteuerungseinrichtung neben den

- prozeßgebundenen Ein- und Ausgängen auch die Verarbeitung der sicherheitsrelevanten Ein- und Ausgänge. Gemäß der Erfindung bezeichnet ein sicherheitsbezogener Eingang eine Informationsquelle, wobei die durch die Quelle abgegebene
- 5 Information in irgendeinem Zusammenhang zur Sicherheit des erfindungsgemäßen Automatisierungssystems steht.
- Beispielsweise ist der Drehzahlsensor einer Drehmaschine, welche über einen Busteilnehmer 32 an den Bus 2 angeschlossen ist, ein derartiger sicherheitsrelevanter Eingang, da die
- 10 Maschine nicht über eine vorgegebene Grenze drehen darf. Ein weiteres Beispiel für einen sicherheitsbezogenen Eingang in der beschriebenen Ausführungsform der Erfindung ist ein Photodetektor einer Lichtschranke, mit welcher der Arbeitsbereich der Drehmaschine überwacht wird. Auch in
- 15 diesem Fall besitzt die Standardsteuerungseinrichtung über den Bus Zugriff auf die Information des sicherheitsbezogenen Eingangs. Nach der Verarbeitung der sicherheitsbezogenen Daten, beispielsweise in Form einer logischen Verknüpfung sendet die Steuerungseinrichtung 4 diese sicherheitsbezogenen
- 20 Verknüpfungsdaten an sicherheitsbezogene Ausgänge.
- Beispielsweise kann die Standardsteuerungseinrichtung einen Abschaltbefehl für die erwähnte Drehmaschine über den Bus zum zugeordneten Busteilnehmer 32 absenden, wenn die Höchstdrehzahl überschritten wurde und damit eine Gefahr
- 25 besteht, daß die Anlage außer Kontrolle gerät. Auch in diesem Fall kommuniziert die sicherheitsbezogene Steuerung in der Standardsteuerungseinrichtung über den Bus mit dem sicherheitsbezogenen Ausgang.
- 30 Das erfindungsgemäße Automatisierungssystem umfaßt ferner zwei Sicherheitsanalysatoren 5, 5', welche jeweils mittels einer Schnittstelle den Datenfluß über das Bussystem in Echtzeit mithören. Die Sicherheitsanalysatoren sind zum



Verknüpfen und/oder Verarbeiten von sicherheitsbezogenen Daten im Busdatenstrom eingerichtet. Dies bedeutet, daß sie sicherheitsbezogene Verknüpfungen der Standardsteuerungseinrichtung nachvollziehen können, da ihnen  
5 die über den Bus transportierten sicherheitsbezogenen Daten zugänglich sind.

Hierzu weisen die Sicherheitsanalysatoren 5, 5' jeweils eine frei programmierbare Logikeinrichtung auf, in welcher die  
10 abgehörten Daten, insbesondere die abgehörten sicherheitsbezogenen Daten verarbeitet werden. Beispielsweise können die Sicherheitsanalysatoren 5, 5' durch Nachbilden der sicherheitsbezogenen Verknüpfungen der Standardsteuerung deren als Ausgangsdaten über den Bus gesendeten  
15 Verknüpfungsdaten überprüfen. In vorliegendem Fall beziehen sich die sicherheitsbezogenen Verknüpfungen auf einen einzelnen Busteilnehmer 32. In diesem Fall ist der Sicherheitsanalysator 5 für die sicherheitsbezogenen Ein- bzw. Ausgänge, welche diesen Busteilnehmer zugeordnet sind,  
20 zuständig. In der in Fig. 1 dargestellten Ausführungsform der Erfindung sind die Sicherheitsanalysatoren 5 bzw. 5' keine logischen Busteilnehmer des Automatisierungssystems. Der Sicherheitsanalysator 5 weist jedoch einen sicherheitsbezogenen Ausgang 6 auf, über welchen der dem  
25 Sicherheitsanalysator zugeordnete Busteilnehmer 32 ausgeschaltet werden kann. Dies geschieht mittels einer Schaltung eines Schützes 7, welcher den Busteilnehmer bzw. die angeschlossenen Baugruppen und Maschinen von der Versorgungsspannung trennt. Auf diese Weise führt der  
30 Sicherheitsanalysator 5 im Ansprechen auf die Überprüfung oder den Vergleich eine sicherheitsbezogene Funktion, hier das Abschalten der Versorgungsspannung aus. Wenn beispielsweise ein Fehler der sicherheitsbezogenen

Verknüpfungsdaten aus der Standardsteuereinrichtung erkannt wird, kann der Sicherheitsanalysator über den beschriebenen Ausgang den betroffenen Busteilnehmer abschalten, da die sicherheitsbezogene Steuerung durch die

5 Standardsteuerungseinrichtung nicht mehr vorgabegemäß arbeitet. In ähnlicher Weise wird ein Busteilnehmer abgeschaltet, wenn die sicherheitsbezogene Steuerung nicht notwendige Daten an den Busteilnehmer sendet und infolgedessen Gefahr besteht, daß die Anlage in einen

10 undefinierten Zustand gerät.

In der beschriebenen Ausführungsform ist über einen Buskoppler 9 ein Lokalbusstich 8 mit drei Busteilnehmern 33, 34 und 35 angeordnet. Diese Busteilnehmer sind von der

15 Funktionfähigkeit und vom Betrieb des Busteilnehmers 32 abhängig, welcher dem Sicherheitsanalysator 5 zugeordnet ist. Demnach ist es notwendig, beim Abschalten des Busteilnehmers 32 auch die Busteilnehmer des Lokalbusstichs 8 von der Versorgungsspannung zu trennen. Diese Verrieglungslogik ist

20 im Sicherheitsanalysator 5 abgelegt. Somit sind insgesamt vier Busteilnehmer mit ihren nachgeordneten Baugruppen und Maschinen abzuschalten, was in Fig. 1 schematisch durch einen Vierfach-Schütz 7 dargestellt ist.

25 Der Sicherheitsanalysator 5' ist wie der erste Sicherheitsanalysator 5 zum Abhören der über den Bus transportierten Daten eingerichtet. Im Gegensatz zum ersten Sicherheitsanalysator 5 weist er jedoch keinen Ausgang auf, mit welchem er sicherheitsbezogene Funktionen ausführen kann.

30 Statt dessen umfaßt er einen sicherheitsbezogenen Eingang 10, über welchen der Sicherheitsanalysator mit einer sicherheitsbezogenen Einrichtung 11 des Automatisierungssystems zur Erfassung von

sicherheitsbezogenen Daten verbunden ist. Im vorliegenden Fall umfaßt diese Einrichtung 11 einen Photodetektor, welcher als Teil einer Lichtschranke den Arbeitsbereich eines Schweißroboters überwacht. Der Sensor ist nicht mittels eines Busteilnehmers an den Automatisierungsbuss angeschlossen, sondern direkt an den Sicherheitsanalysator 5'. Im Ansprechen auf die über den sicherheitsbezogenen Eingang 10 des Sicherheitsanalysators 5' erfaßten sicherheitsbezogenen Daten führt auch hier der Sicherheitsanalysator eine sicherheitsbezogene Funktion aus. Wird durch den Photodetektor 11 das Eindringen einer Person in den Arbeitsbereich des Roboters erfaßt, so schaltet der Sicherheitsanalysator 5' den entsprechenden Busteilnehmer 38 und seine zugeordneten Baugruppen und den Roboter selbst aus. Hierzu weist der Sicherheitsanalysator 5' eine Einrichtung zum Manipulieren der auf den Bus übertragenen Eingangs- und Ausgangsdaten auf. Dabei kann zumindest ein Datum des Datenstroms überschrieben, gelöscht und/oder zumindest ein Datum in den Busdatenstrom eingefügt werden. Ein derartiger Vorgang ist in den Fig. 6a und 6b veranschaulicht. Diese Figuren zeigen das Verändern von Eingangs- bzw. Ausgangsdaten der Standardsteuereinrichtung 4 durch den Sicherheitsanalysator 5'. In beiden Fällen wird eine Informationseinheit 12 in einen Speicher des Sicherheitsanalysators eingelesen und daraufhin an die entsprechende Stelle des Datenstroms eine aus einem anderen Speicher des Sicherheitsanalysators entnommene Informationseinheit eingeschrieben. Die Abschaltung des Busteilnehmers und der daran angeschlossenen Baugruppen und damit des Roboters kann sowohl über die Manipulation der Eingangsdaten als auch über die Manipulation der Ausgangsdaten der Standardsteuereinrichtung vorgenommen werden. Wird beispielsweise der Eingangsdatenstrom derartig

verändert, daß der Standardsteuerungseinrichtung 4 ein Betriebsparameter außerhalb der vorgegebenen Grenzen gemeldet wird, so schaltet die Standardsteuerungseinrichtung über den Bus mittels eines dem bestimmten Busteilnehmer 38  
5 übermittelten sicherheitsbezogenen Verknüpfungsdatums diesen Busteilnehmer und damit den Schweißroboter ab. In gleicher Weise kann der Sicherheitsanalysator eine Freigabe durch Standardsteuereinrichtung mittels Überschreiben des entsprechenden Ausgangsdatums rückgängig machen.

10

Fig. 6b zeigt den Fall, daß der Sicherheitsanalysator den Ausgangsdatenstrom auf dem Bus verändert. In diesem Fall manipuliert der Sicherheitsanalysator die an den Busteilnehmer 38 gesendeten Daten derartig, daß der  
15 Busteilnehmer seinen Ausgang und damit auch den Schweißroboter abschaltet.

Fig. 2 zeigt eine weitere Ausführungsform der Erfindung. Dabei ist der Bus ein nach dem Master-Slave-Prinzip  
20 arbeitendes System, wobei die Standardsteuerungseinrichtung als Master und die einzelnen Busteilnehmer als Slaves fungieren. Das Bussystem ist über eine Anschaltbaugruppe 41 mit einem Host 40 verbunden, wobei die prozeßbezogene Steuerung im Host und die sicherheitsbezogene Steuerung in  
25 der Anschaltbaugruppe angeordnet ist bzw. abläuft. Die Anlage umfaßt einen einzelnen Sicherheitsanalysator 5, der direkt hinter die Anschaltbaugruppe zum Abhören des Busdatenstroms an dem Bus angekoppelt ist. Durch diese Maßnahme wird sichergestellt, daß der Sicherheitsanalysator an dem  
30 seriellen Bus mit Ringstruktur den gesamten Eingangs- als auch den gesamten Ausgangs-Datenstrom auf dem Bus abhören kann. Aufgrund der Erkenntnis des gesamten Datenstroms über den Bus legt der Sicherheitsanalysator 5 in der beschriebenen

Ausführungsform ein vollständiges Prozeßabbild in einem dafür vorgesehenen Speicher ab. Demzufolge ist der Sicherheitsanalysator in der Lage, die Gesamtheit der sicherheitsbezogenen Verknüpfungsdaten der

5 sicherheitsbezogenen Steuerung in der Anschaltbaugruppe zu überprüfen und bei Bedarf, d.h. beim Auftreten eines Fehlers, den Ausgang 6 zum Abschalten der Gesamtanlage mittels des Schützes 7 sicherheitsgerichtet derart anzusteuern, daß die Versorgungsspannung für die Gesamtanlage ausgeschaltet wird.

10 Eine Modifikation der in Fig. 2 dargestellten Ausführungsform zeigt das erfindungsgemäße Automatisierungssystem in Fig. 3. Der Sicherheitsanalysator 5 ist hier in die Anschaltbaugruppe 41 integriert. Die sicherheitsbezogene Steuerung der

15 Standardsteuerungseinrichtung als auch die sicherheitsbezogene Datenverarbeitung des Sicherheitsanalysators laufen in der Anschaltbaugruppe in getrennten und unabhängigen Logikbausteinen ab. Weiterhin ist ein zweiter Sicherheitsanalysator 5'' am Kopf des

20 Lokalbusstichs 8 angeordnet. Diese Anordnung bedingt wiederum, daß der Sicherheitsanalysator 5'' die Gesamtheit aller Eingangs- als auch der Ausgangsdaten für die Busteilnehmer 33, 34 und 35 des Lokalbusstich 8 abhören kann und demgemäß ein vollständiges Prozeßabbild für den

25 Prozeßablauf innerhalb des Lokalbusstichs anzulegen. Der Sicherheitsanalysator 5'' ist somit wie der Sicherheitsanalysator 5 im Fernbus-Abschnitt in der Lage, die Gesamtheit der sicherheitsbezogenen Verknüpfungsdaten der sicherheitsbezogenen Steuerung für den Lokalbusabschnitt in

30 der Anschaltbaugruppe zu überprüfen und bei Bedarf wie oben stehend beschrieben, über eine Datenmanipulation die notwendigen sicherheitsbezogenen Funktionen auszulösen. Auf diese Weise lassen sich höchste Sicherheitsanforderungen, die

an die im Busstich 8 vorliegenden sicherheitsrelevanten Ein- und Ausgänge gestellt sind, erfüllen, da der Lokalbusstich 8 sowohl durch die sicherheitsbezogene Steuerung der Standardsteuereinrichtung als auch durch den  
5 Sicherheitsanalysator 5 und durch den Sicherheitsanalysator 5' abgesichert ist.

Eine weitere Ausführungsform der Erfindung zeigt Fig. 4. Das erfindungsgemäße Automatisierungssystem umfaßt zwei  
10 Sicherheitsanalysatoren 5 und 5', deren sicherheitsbezogenen Ausgänge 6 und 6' miteinander gekoppelt sind. Beide Ausgänge steuern eine Vielfach-Schützeinrichtung 7 zum Abschalten der Versorgungsspannung für das Gesamtsystem. Die Anlage wird durch eine Standardsteuerungseinrichtung 4 über den seriellen  
15 Bus 2 gesteuert. Der Sicherheitsanalysator 5 kann aufgrund seiner Anordnung im System die Gesamtheit aller Eingangs- und Ausgangsdaten auf dem Bus abhören, ausgenommen die Eingangsdaten des ersten Busteilnehmers 31, der zwischen der Steuerungseinrichtung 4 und dem Sicherheitsanalysator 5  
20 angeordnet ist. Der Sicherheitsanalysator 5' kann alle Eingangsdaten am Bus abhören, alle Ausgangsdaten außer die für den letzten Busteilnehmers sind ihm jedoch nicht zugänglich. Der erste Sicherheitsanalysator 5 ist deshalb durch Umkopieren der betreffenden Daten im Busdatenfluß in  
25 der Lage, die ihm zugänglichen Ausgangsdaten in Eingangsdaten umzukopieren und somit die dem Sicherheitsanalysator 5' eigentlich nicht zugänglichen Ausgangsdaten zum Anlegen eines Prozeßabbildes für den abzusichernden sicherheitsbezogenen Busteilnehmer 32 auch dem Sicherheitsanalysator 5' verfügbar  
30 zu machen. Da beide Sicherheitsanalysatoren dieselbe Eingangsinformation erhalten, können sie sich im Hinblick auf die sicherheitsbezogenen Ein- bzw. Ausgänge des abzusichernden Busteilnehmers 32 überwachen. Auf diese Weise

ist eine verteilte Redundanz der Sicherheitstechnik im  
erfindungsgemäßen Automatisierungssystem realisiert. Im  
vorliegenden Beispiel weist der Sicherheitsanalysator 5'  
weiterhin einen sicherheitsbezogenen Eingang 10 auf, an  
5 welchen ein Notschalter 13 angeschlossen ist. Auf das  
Schließen des Notschalters 13 spricht der  
Sicherheitsanalysator 5' mit der im Sicherheitsanalysator  
zugeordneten sicherheitsbezogenen Funktion an, nämlich dem  
Öffnen des Schützes 7 zur Abschaltung der Gesamtanlage.

10

Das beschriebene Verfahren des Umkopierens von Eingangsdaten  
in Ausgangsdaten und umgekehrt wird erfindungsgemäß auch dazu  
benutzt, um eine Datenverbindung in dem nach dem Master-  
Slave-Prinzip arbeitenden Automatisierungssystem zwischen  
15 zwei Slaves zu realisieren ohne daß der Master für die  
Datenübermittlung benötigt wird. Hierbei kann beispielsweise  
ein einem Busteilnehmer zugeordneter Sicherheitsanalysator  
das zu übermittelnde Datum des Busteilnehmers in den  
Eingangs-Datenstrom einfügen und somit einem nachfolgenden  
20 Busteilnehmer ohne die Beanspruchung des Masters zur  
Verfügung stellen. Auf diese Weise läßt sich bei Bedarf auch  
auf einfache Weise ein Multi- oder Broadcast der Information  
zu allen übrigen nachfolgenden Busteilnehmern verwirklichen.

25 In einer nichtdargestellten Ausführungsform der Erfindung ist  
der Sicherheitsanalysator in einem zugeordneten  
sicherheitsgerichteten Busteilnehmer integriert. Die  
sicherheitsgerichteten Verknüpfungen laufen dabei in einer  
Logikeinheit des Busteilnehmers ab, somit läßt sich im  
30 Busteilnehmer eingebaute Intelligenz für die  
sicherheitsgerichteten Verknüpfungen nutzen. Da der  
Busteilnehmer eine Busschnittstelle aufweist, verringert sich  
der zusätzliche Hardwareaufwand für den Sicherheitsanalysator

beträchtlich.

Bei der Datenübertragung in den beschriebenen  
 erfindungsgemäßen Automatisierungssystemen werden zumindest  
 5 teilweise die sicherheitsbezogenen Daten in einem  
 Sicherheitsprotokoll über den Bus übertragen. Dieses  
 Sicherheitsprotokoll kann je nach Anforderung zusätzlich zum  
 Sicherheitsdatum das negierte Sicherheitsdatum, eine Adresse  
 und/oder eine Datensicherungsinformation in Form eines CRC  
 10 umfassen. Auf diese Weise lassen sich Fehler bei der  
 Datenübertragung leicht erkennen. Zu diesem Zweck wird ein im  
 erfindungsgemäßen Automatisierungssystem verwendeter  
 Sicherheitsanalysator derartig eingerichtet, daß er das  
 Sicherheitsprotokoll lesen und entsprechend auswerten kann.

15 Mittels der im Sicherheitsprotokoll übertragene Adresse des  
 Sicherheitsbusteilnehmers kann der Sicherheitsanalysator bei  
 geändertem Busaufbau, beispielsweise durch  
 sicherheitsbezogene Abschaltung der Komponente, eine  
 20 Anpassung der Programmierung vornehmen bzw. den Datensatz des  
 ihm zugeordneten Teilnehmers erkennen und die Veränderung des  
 Busaufbaus berücksichtigen. Zusätzlich kann durch die  
 Aufnahme der Adresse in das Sicherheitsprotokoll ein  
 Ablagefehler durch einen Busfehler oder einen Ausfall einer  
 25 dezentralen Einheit erfaßt werden.

Eine besondere Ausführungsform eines Sicherheitsanalysators  
 zur Verwendung im erfindungsgemäßen Automatisierungssystem  
 zeigt Fig. 5. Der dargestellte Sicherheitsanalysator 5 weist  
 30 sowohl 4 sicherheitsgerichtete Eingänge 10 zur Erfassung  
 sicherheitsgerichteter Information von Photodetektoren 11 als  
 auch 4 sicherheitsgerichtete Ausgänge 6 zum Abschalten der  
 Versorgungsspannung von 4 Automatisierungsbuskomponenten



durch Schütze auf. Die verschiedenen sicherheitsgerichteten Ausgänge 6 werden dabei im Ansprechen auf die im Sicherheitsanalysator ablaufenden Verknüpfungen, den Vergleich mit sicherheitsgerichteten Verknüpfungen der Standardsteuerung und/oder eine sicherheitsbezogene Eingangsinformation über den Eingang 10 angesteuert. Hierbei ist eine Verrieglungslogik im Sicherheitsanalysator abgelegt, die vorgibt, welche sicherheitsgerichteten Funktionen beim Auftreten eines bestimmten Fehlers ausgelöst werden, d.h. welche Komponenten beim Auftreten des Fehlers von der Versorgungsspannung abgetrennt werden müssen.

Es liegt im Rahmen der Erfindung, daß ein Sicherheitsanalysator neben der Verarbeitung von sicherheitsbezogenen Daten auch eine Prozeßdatenverarbeitung durchführt.

Weiterhin ist festzuhalten, daß das Prinzip der Erfindung nicht auf die in den Ausführungsbeispielen dargestellten Automatisierungsbussysteme beschränkt ist, sondern statt dessen auf alle Automatisierungsanlagen mit einem Bus angewendet werden kann.

Patentansprüche:

- 5 1. Automatisierungssystem (1), zumindest umfassend
  - ein Bussystem (2), daran
  - angeschlossene E/A-Busteilnehmer (31-38) und eine Standardsteuerungseinrichtung (4; 40, 41), sowie wenigstens
  - 10 - einen Sicherheitsanalysator (5, 5', 5''), welcher den Datenfluß über das Bussystem mithört und zum Ausführen zumindest einer sicherheitsbezogenen Funktion ausgebildet ist, dadurch gekennzeichnet, daß
  - 15 die Standardsteuerungseinrichtung zumindest einen sicherheitsbezogenen Ausgang steuert und daß der Sicherheitsanalysator zum Überprüfen und/oder Verarbeiten von sicherheitsbezogenen Daten im Busdatenstrom eingerichtet ist.
  - 20
2. Automatisierungssystem (1) nach Anspruch 1, dadurch gekennzeichnet, daß der Sicherheitsanalysator (5, 5', 5'') eine frei programmierbare Logikeinrichtung aufweist, welche die abgehörten Daten, insbesondere die
- 25 abgehörten sicherheitsbezogenen Daten verarbeitet.
3. Automatisierungssystem (1) nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß
- 30 der Sicherheitsanalysator (5, 5', 5'') kein logischer Busteilnehmer des Automatisierungssystems (1) ist und dieser zumindest einen sicherheitsbezogenen Ausgang (6) aufweist, über welchen wenigstens eine dem Sicherheitsanalysator zugeordnete Baugruppe des

Automatisierungssystem, insbesondere wenigstens ein Busteilnehmer (31-38), ein- oder ausschaltbar ist.

4. Automatisierungssystem (1) nach Anspruch 3,  
5 dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5, 5', 5'') zur Abschaltung  
einer Sicherheitsinsel, eines Busstichs (8) und/oder der  
Gesamtanlage eingerichtet ist.
- 10 5. Automatisierungssystem (1) nach einem der Ansprüche 1  
bis 4, dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5') zumindest einen  
sicherheitsbezogenen Eingang (10) aufweist, über welchen  
der Sicherheitsanalysator mit einer sicherheitsbezogenen  
15 Einrichtung (11) des Automatisierungssystem zur  
Erfassung von sicherheitsbezogenen Daten verbunden ist.
6. Automatisierungssystem (1) nach einem der Ansprüche 1  
bis 5, dadurch gekennzeichnet, daß  
20 das Bussystem (2) über eine Anschaltbaugruppe (41) mit  
einem Host (40) verbunden ist,  
wobei die prozeßbezogene Steuerung im Host und die  
sicherheitsbezogene Steuerung in der Anschaltbaugruppe  
angeordnet ist.  
25
7. Automatisierungssystem (1) nach einem der Ansprüche 1  
bis 6, dadurch gekennzeichnet, daß  
der Bus (2) ein serieller Bus ist und zumindest ein  
Sicherheitsanalysator (5, 5') im Fernbus-Abschnitt des  
30 Automatisierungssystem angeordnet ist.
8. Automatisierungssystem (1) nach Anspruch 7,  
dadurch gekennzeichnet, daß

ein Sicherheitsanalysator (5) direkt nach dem Host (40) oder der Anschaltbaugruppe (41) angeordnet ist.

- 5 9. Automatisierungssystem (1) nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß ein Sicherheitsanalysator (5) in der Anschaltbaugruppe (41) angeordnet ist.
- 10 10. Automatisierungssystem (1) nach einem der vorstehenden Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der Sicherheitsanalysator (5, 5', 5'') eine Speichereinrichtung zum Anlegen eines Prozeßabbildes umfaßt.
- 15 11. Automatisierungssystem (1) nach einem der vorstehenden Ansprüche 1 bis 10, dadurch gekennzeichnet, daß der Sicherheitsanalysator (5, 5', 5'') eine Einrichtung zum Manipulieren des auf dem Bus (2) übertragene  
20 Datenstroms, insbesondere der Eingangs- und/oder Ausgangsdaten, aufweist.
- 25 12. Automatisierungssystem (1) nach Anspruch 11, dadurch gekennzeichnet, daß die Einrichtung Eingangs- und/oder Ausgangsdaten überschreibt und/oder Daten in den Datenstrom einfügt.
- 30 13. Automatisierungssystem (1) nach einem der vorstehenden Ansprüche 1 bis 12, dadurch gekennzeichnet, daß zumindest ein Sicherheitsanalysator (5, 5', 5'') redundant aufgebaut ist.

14. Verfahren zum Betrieb einer Automatisierungssystems, insbesondere eines Automatisierungssystems (1) nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, daß durch die
- 5 Standardsteuerungseinrichtung (4; 40, 41) die Prozeßsteuerung mit der Verarbeitung von prozeßgebundenen E/A-Daten und eine sicherheitsbezogene Steuerung mit der Verarbeitung von sicherheitsbezogenen Daten durchgeführt wird und weiterhin eine Verarbeitung
- 10 sicherheitsbezogener Daten auf zumindest einem Sicherheitsanalysator (5, 5', 5'') durchgeführt wird, wobei im Sicherheitsanalysator sicherheitsbezogene Daten, insbesondere sicherheitsbezogene Verknüpfungsdaten im Busdatenstrom verarbeitet werden.
- 15
15. Verfahren nach Anspruch 14, dadurch gekennzeichnet, daß in einem Sicherheitsanalysator (5, 5', 5'') ein Vergleich der über den Bus übertragenen
- 20 sicherheitsbezogenen Verknüpfungsdaten der Standardsteuerungseinrichtung (4, 41) und/oder zumindest eines weiteren Sicherheitsanalysators (5, 5', 5'') mit den entsprechenden Verknüpfungsdaten des ersten Sicherheitsanalysators durchgeführt wird.
- 25
16. Verfahren nach einem der Ansprüche 14 oder 15, dadurch gekennzeichnet, daß die durch die Standardsteuerung (4, 41) erzeugten und als Ausgangsdaten über den Bus gesendeten
- 30 Verknüpfungsdaten in zumindest einem Sicherheitsanalysator (5, 5', 5'') durch Nachbilden der sicherheitsbezogenen Verknüpfungen der Standardsteuerung (4, 41) überprüft werden.

17. Verfahren nach einem der Ansprüche 14 bis 16,  
dadurch gekennzeichnet, daß  
im Ansprechen auf die Überprüfung oder den Vergleich  
5 durch den Sicherheitsanalysator (5, 5', 5'')  
sicherheitsbezogene Funktionen ausgeführt werden.
18. Verfahren nach einem der Ansprüche 14 bis 17,  
dadurch gekennzeichnet, daß  
10 im Ansprechen auf die über den sicherheitsbezogenen  
Eingang (10) des Sicherheitsanalysators (5') erfaßten  
sicherheitsbezogenen Daten der Sicherheitsanalysator  
sicherheitsbezogene Funktionen ausführt.
- 15 19. Verfahren nach Anspruch 18,  
dadurch gekennzeichnet, daß  
das Ausführen einer sicherheitsbezogenen Funktion das  
Ein- oder Ausschalten zumindest einer Baugruppe des  
Automatisierungsbussystems, insbesondere eines  
20 Busteilnehmers (32-38) umfaßt.
20. Verfahren nach einem der Ansprüche 14 bis 19,  
dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5', 5'') mittels einer  
25 Einrichtung zum Manipulieren des Datenstroms auf dem Bus  
(2) zumindest ein Datum des Datenstroms überschreibt,  
löscht und/oder zumindest ein Datum in den Bus-  
Datenstrom einfügt.
- 30 21. Verfahren nach der Anspruch 20,  
dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5, 5', 5'') den abgehörten  
Datenstrom zumindest teilweise abspeichert und

Eingangsdaten des Bus-Datenstroms in Ausgangsdaten des Bus-Datenstroms, und umgekehrt, umkopiert.

22. Verfahren nach einem der Ansprüche 14 bis 21,  
5 dadurch gekennzeichnet, daß  
sicherheitsbezogenen Daten in einem  
Sicherheitsprotokoll über den Bus (2) übertragen  
werden.
- 10 23. Verfahren nach Anspruch 22,  
dadurch gekennzeichnet, daß  
das Sicherheitsprotokoll zusätzlich zum Sicherheitsdatum  
das negierte Sicherheitsdatum, eine laufende Nummer,  
eine Adresse und/oder eine Datensicherungsinformation  
15 (CRC) umfaßt.
24. Verfahren nach einem der Ansprüche 14 bis 23,  
dadurch gekennzeichnet, daß  
20 der Bus ein nach dem Master-Slave-Prinzip arbeitendes  
System ist, wobei Daten zwischen zumindest zwei Slaves,  
insbesondere zwischen einzelnen Busteilnehmern (31-38),  
mittels einer Daten-Verbindung über wenigstens einen  
Sicherheitsanalysator (5, 5', 5'') übertragen werden,  
wobei der Sicherheitsanalysator Daten im Busdatenstrom  
25 umkopiert.
25. Verfahren nach einem der Ansprüche 14 bis 23,  
dadurch gekennzeichnet, daß  
30 der Bus ein nach dem Master-Slave-Prinzip arbeitendes  
System ist, wobei Daten zwischen zumindest zwei Slaves,  
insbesondere zwischen einzelnen Busteilnehmern (31-38),  
mittels einer Daten-Verbindung über die Steuerung oder  
den Master übertragen werden, wobei die Steuerung bzw.

der Master Daten im Busdatenstrom umkopiert.

26. Verfahren nach einem der Ansprüche 14 bis 25,  
dadurch gekennzeichnet, daß
- 5       mittels eines Sicherheitsanalysators (5, 5', 5'')  
Qualitätsdaten erzeugt und/oder eine Aufbereitung der  
gelesenen Daten zur weiteren Verarbeitung durchgeführt  
werden.
- 10   27. Verfahren nach einem der Ansprüche 14 bis 26,  
dadurch gekennzeichnet, daß  
die in einem Sicherheitsanalysator (5') ablaufenden  
sicherheitsbezogenen Verknüpfungen zumindest teilweise  
redundant in wenigstens einem weiteren
- 15       Sicherheitsanalysator (5'') durchgeführt und durch beide  
Sicherheitsanalysatoren zumindest teilweise die  
gleichen Sicherheitsfunktionen ausgeführt werden.
28. Verfahren nach einem der Ansprüche 14 bis 27,  
dadurch gekennzeichnet, daß
- 20       ein Sicherheitsanalysator zumindest teilweise auch eine  
Prozeßdatenverarbeitung durchführt.



Zusammenfassung

Die Erfindung betrifft ein sicherheitsbezogenes  
Automatisierungssystem und ein Verfahren zum Betrieb eines  
5 derartigen Systems.

Um ein sicherheitsbezogenes Automatisierungsbussystem  
bereitzustellen, welches mit einer geringen Hardware-  
Redundanz auskommt und flexibel an die jeweiligen  
Anfordernisse angepaßt werden kann, umfaßt das  
10 Automatisierungssystem zumindest einen Sicherheitsanalysator,  
der mittels einer Schnittstelle an den Bus angeschlossen ist  
und den Datenfluß über den Bus mithört, wobei der Analysator  
zum Ausführen von sicherheitsbezogenen Funktionen  
eingerichtet ist. Das Automatisierungssystem zeichnet sich  
15 dadurch aus, daß die Standardsteuereinrichtung zumindest  
einen sicherheitsbezogenen Ausgang ansteuert und der  
Sicherheitsanalysator zur Überprüfung und/oder zum  
Verarbeiten von sicherheitsbezogenen Daten im Busdatenstrom  
ausgebildet ist.

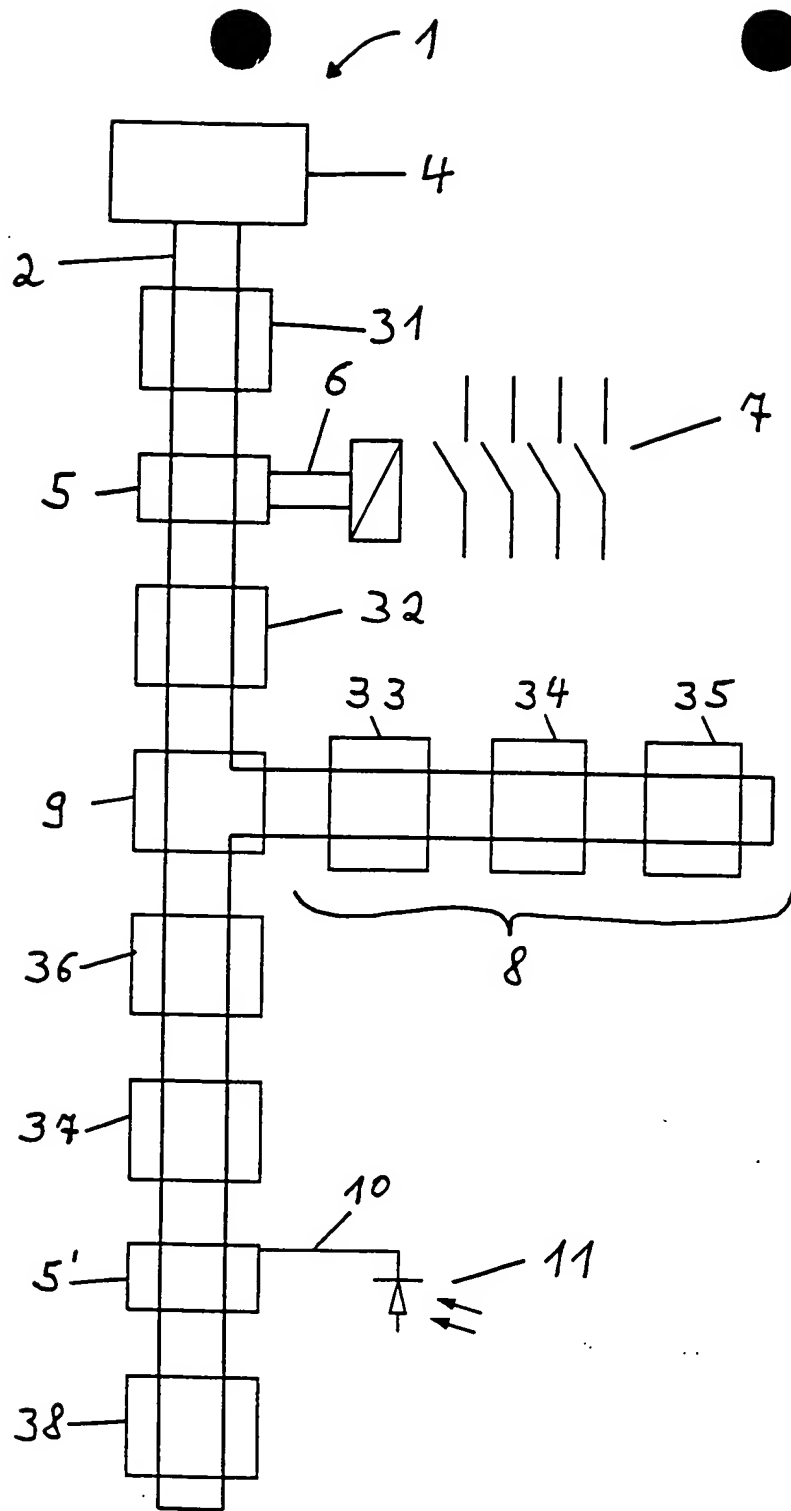


Fig. 1

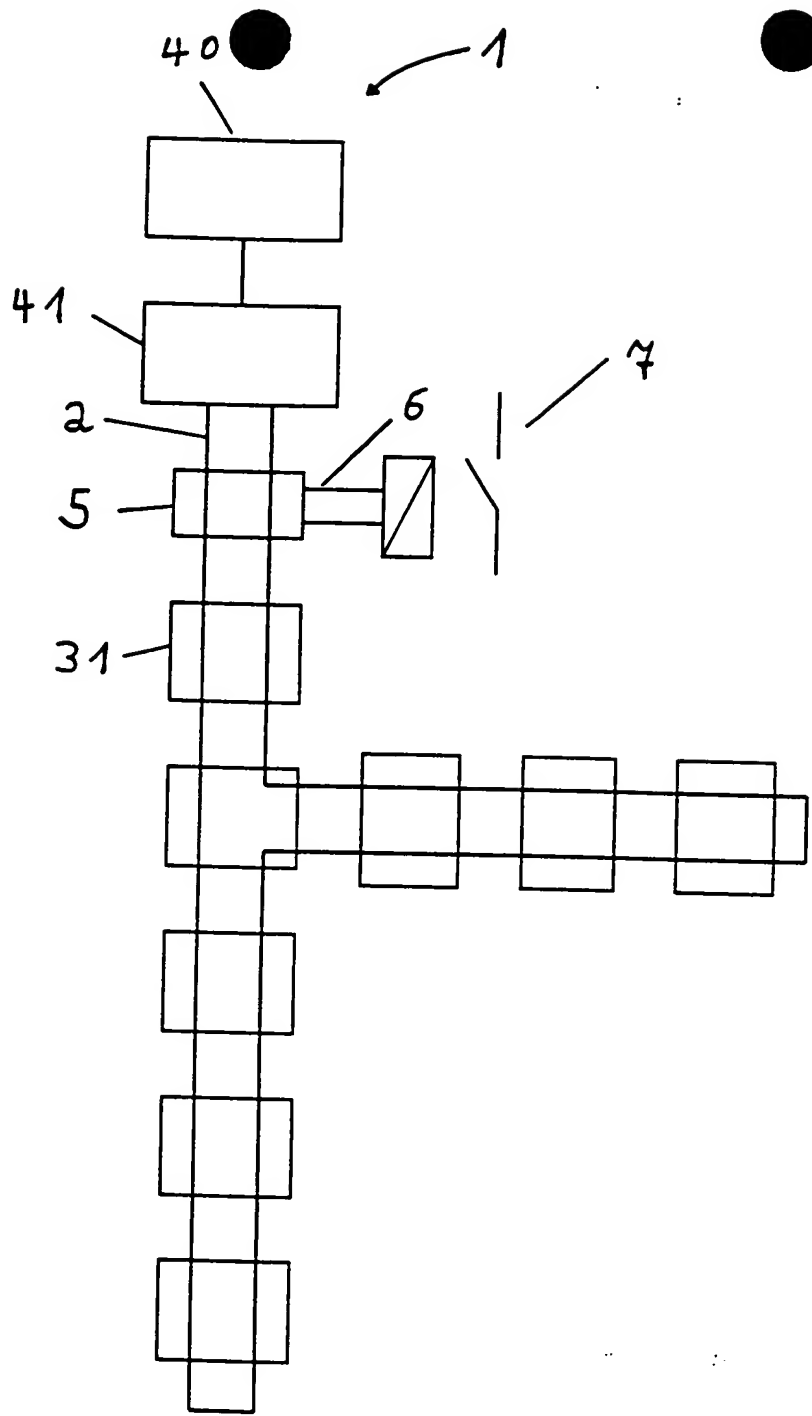


Fig. 2

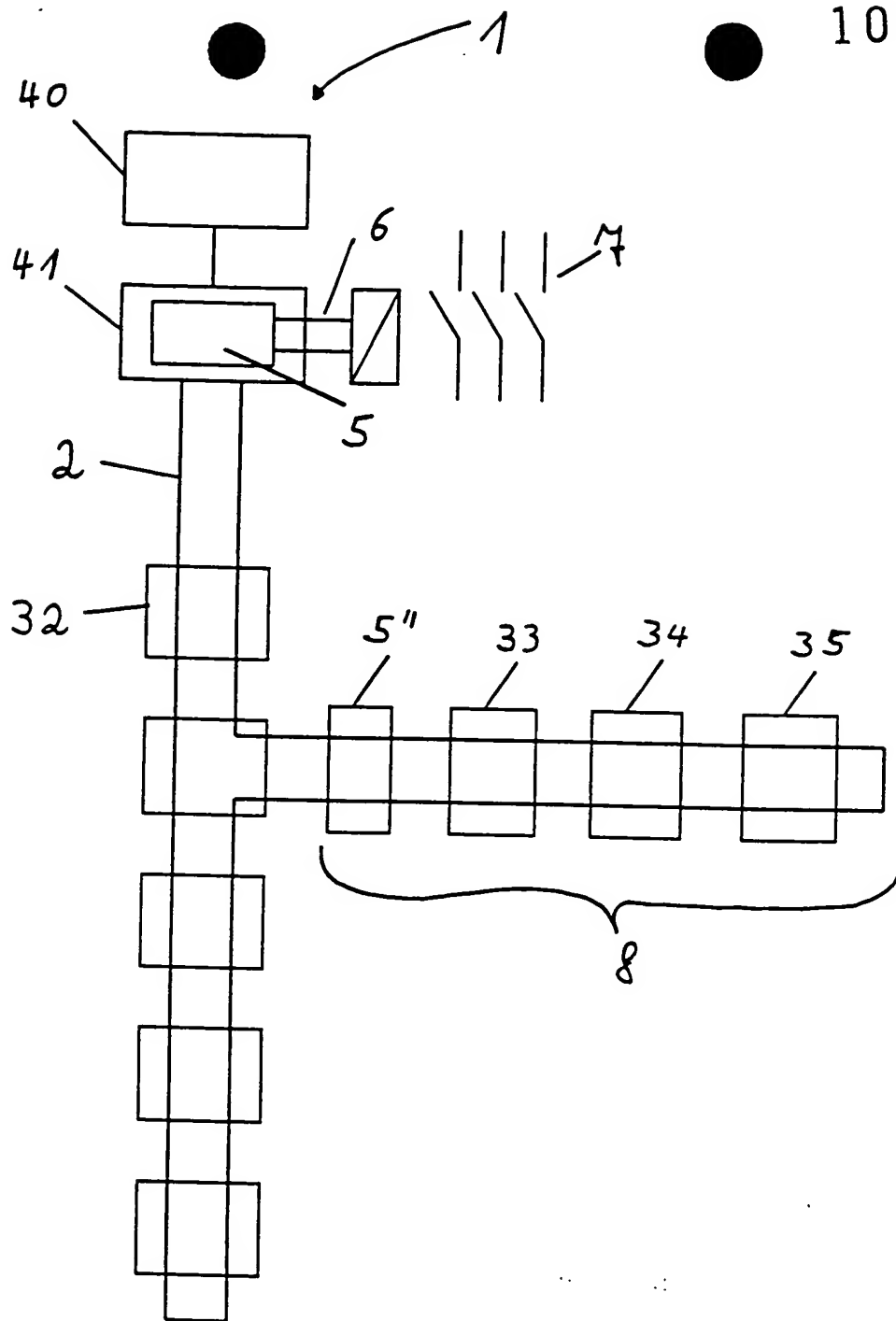


Fig. 3

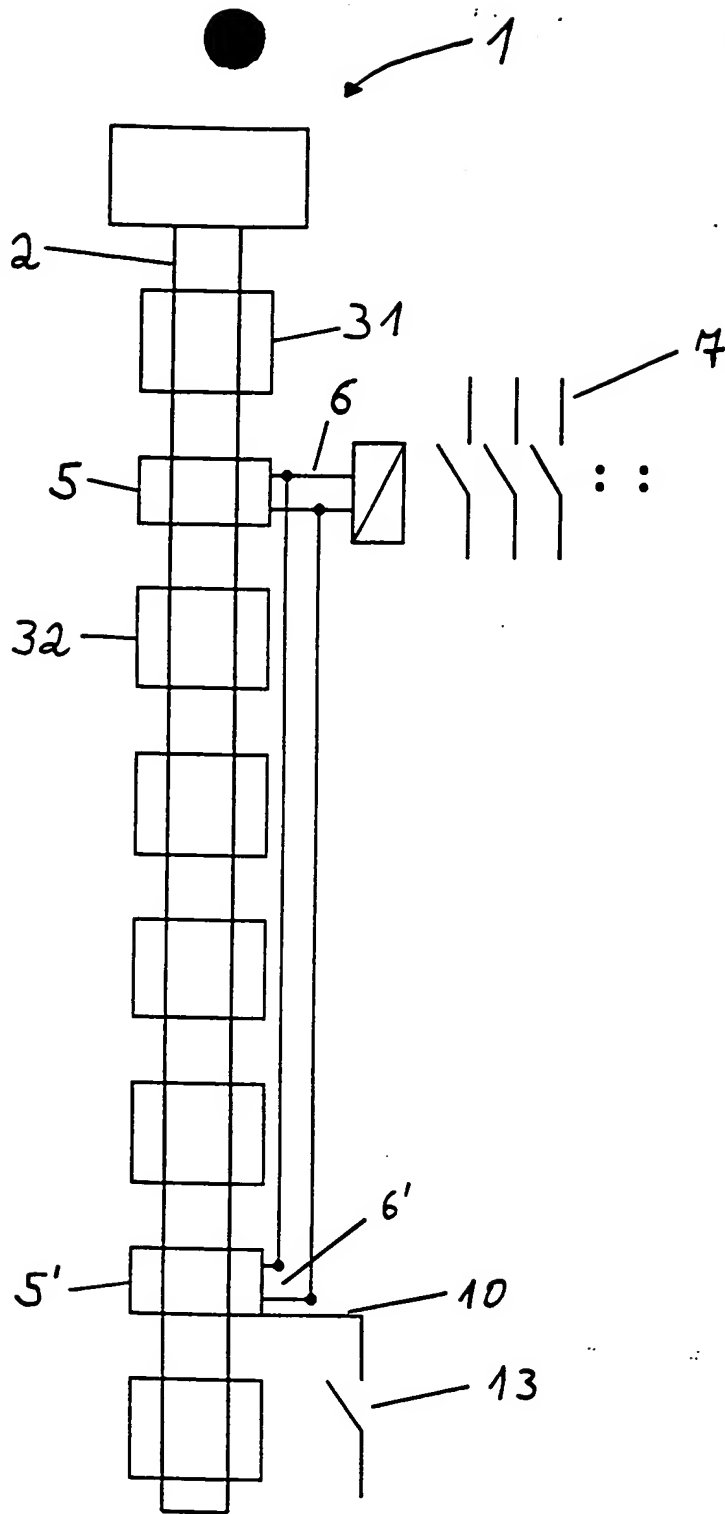
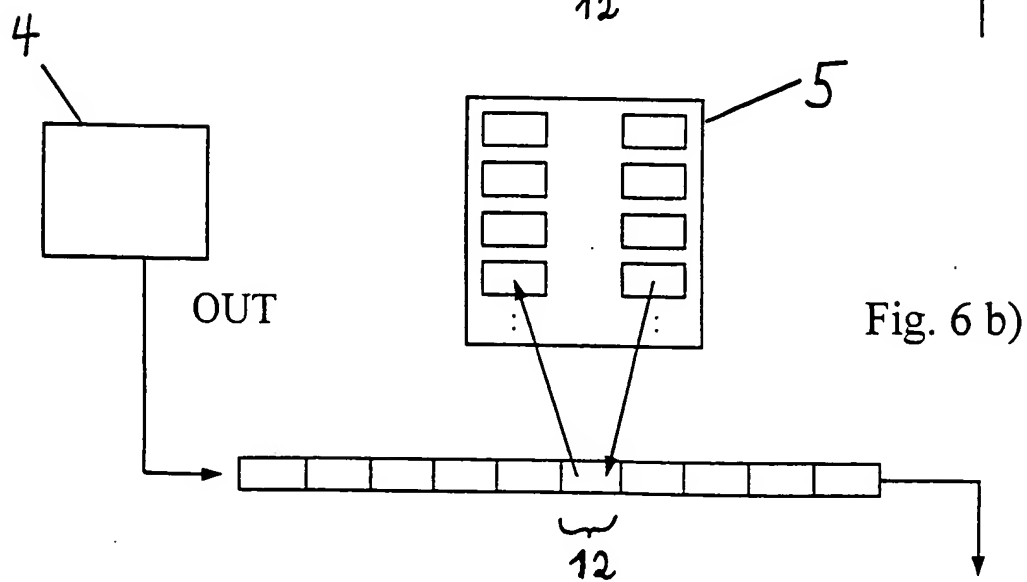
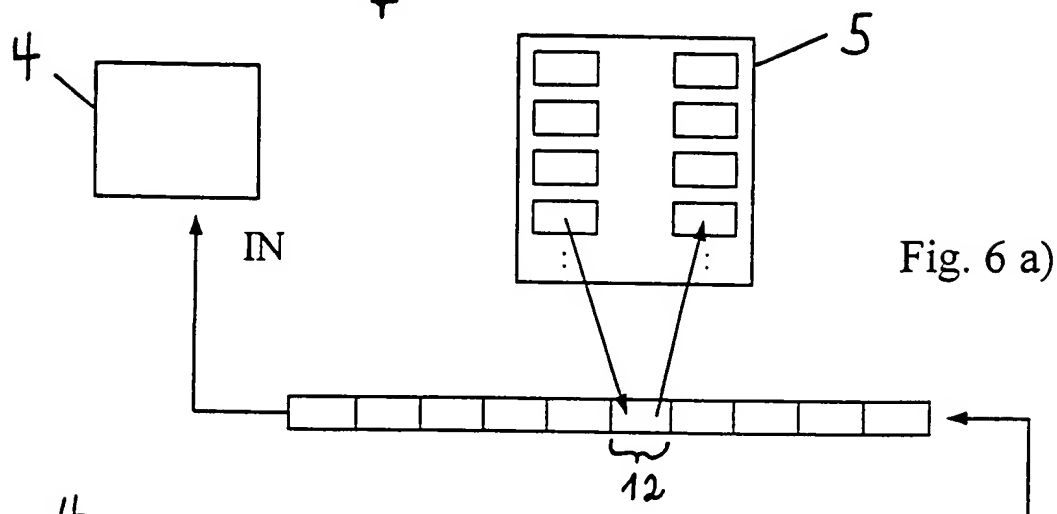
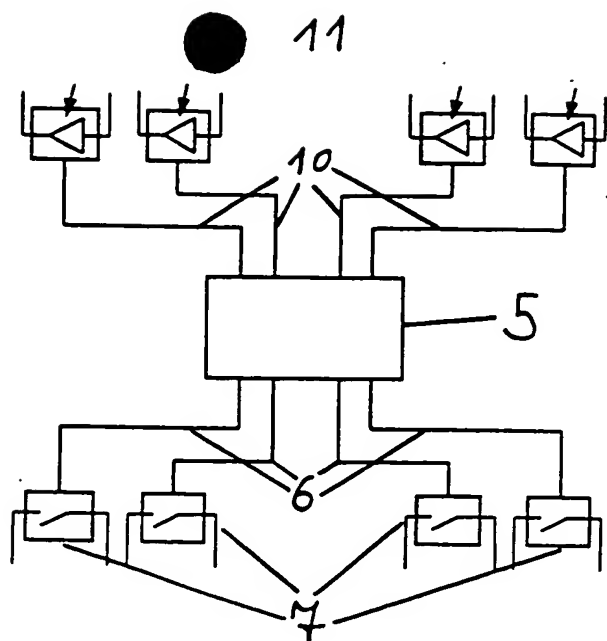


Fig. 4





# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENSARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

### INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>OOPH 0259WOP</b>		<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen <b>PCT/DE00/01901</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>16/06/2000</b>	Prioritätsdatum (Tag/Monat/Jahr) <b>17/06/1999</b>	
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK <b>G05B19/042</b>			
Anmelder <b>PHOENIX CONTACT GMBH &amp; CO. KG et al.</b>			
<p>1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.</p> <p>2. Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.</p> <p><input checked="" type="checkbox"/> Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).</p> <p>Diese Anlagen umfassen insgesamt 8 Blätter.</p>			
<p>3. Dieser Bericht enthält Angaben zu folgenden Punkten:</p> <ul style="list-style-type: none"> <li>I <input checked="" type="checkbox"/> Grundlage des Berichts</li> <li>II <input type="checkbox"/> Priorität</li> <li>III <input type="checkbox"/> Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit</li> <li>IV <input type="checkbox"/> Mangelnde Einheitlichkeit der Erfindung</li> <li>V <input checked="" type="checkbox"/> Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung</li> <li>VI <input type="checkbox"/> Bestimmte angeführte Unterlagen</li> <li>VII <input checked="" type="checkbox"/> Bestimmte Mängel der internationalen Anmeldung</li> <li>VIII <input checked="" type="checkbox"/> Bestimmte Bemerkungen zur internationalen Anmeldung</li> </ul>			
Datum der Einreichung des Antrags  <b>09/01/2001</b>		Datum der Fertigstellung dieses Berichts  <b>07.09.2001</b>	
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:   Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465		Bevollmächtigter Bediensteter  <b>Jonda, S</b>  Tel. Nr. +49 89 2399 2175 	

**INTERNATIONALER VORLÄUFIGER  
PRÜFUNGSBERICHT**Internationales Aktenzeichen **PCT/DE00/01901****I. Grundlage des Berichts**

1. Hinsichtlich der Bestandteile der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):  
**Beschreibung, Seiten:**

1-23 ursprüngliche Fassung

**Patentansprüche, Nr.:**

1-31 eingegangen am 17/08/2001 mit Schreiben vom 14/08/2001

**Zeichnungen, Blätter:**

1/5-5/5 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:



**INTERNATIONALER VORLÄUFIGER  
PRÜFUNGSBERICHT**Internationales Aktenzeichen **PCT/DE00/01901**

- ☐ Beschreibung,      Seiten:  
☐ Ansprüche,      Nr.:  
☐ Zeichnungen,      Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

*(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).*

6. Etwaige zusätzliche Bemerkungen:

**V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

**1. Feststellung**

Neuheit (N)	Ja: Ansprüche	1-14, 16-31
	Nein: Ansprüche	15
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-14, 23
	Nein: Ansprüche	16-22, 24-31
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-31
	Nein: Ansprüche	

- 2. Unterlagen und Erklärungen**  
**siehe Beiblatt**

**VII. Bestimmte Mängel der internationalen Anmeldung**

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:  
**siehe Beiblatt**

**VIII. Bestimmte Bemerkungen zur internationalen Anmeldung**

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:  
**siehe Beiblatt**

**INTERNATIONALER VORLÄUFIGER  
PRÜFUNGSBERICHT - BEIBLATT**

Internationales Aktenzeichen PCT/DE00/01901

**Sektion V**

Zur Prüfung wurden folgende Druckschriften als relevanter Stand der Technik herangezogen:

- D1: DE 198 15 150 A (LEUZE ELECTRONIC GMBH & CO) 22. Oktober 1998 (1998-10-22)  
D2: EP 0 770 942 A (ELAN SCHALTELEMENTE GMBH) 2. Mai 1997 (1997-05-02)  
D3: MOHLENBEIN H: "INTERBUS-DEZENTRALE ECHTZEIT-PERIPHERIE FÜR STANDARD-SPS-SYSTEME" ELEKTRIE, DD, VEB VERLAG TECHNIK. BERLIN, Bd. 44, Nr. 7, 1990, Seiten 244-249, XP000162759 ISSN: 0013-5399  
D4: US 4 680 753 A (FULTON TEMPLE L ET AL) 14. Juli 1987 (1987-07-14)  
D5: EP 0 837 394 A (ELAN SCHALTELEMENTE GMBH) 22. April 1998 (1998-04-22)  
D6: DE 195 10 470 A (KLASCHKA IND ELEKTRONIK) 17. Oktober 1996 (1996-10-17)  
D7: EP 0 600 311 A (SQUARE D DEUTSCHLAND) 8. Juni 1994 (1994-06-08)

1. Dokument D1 zeigt in Fig. 1 ein Automatisierungssystem, zumindest umfassend
- ein Bussystem (1), daran
  - angeschlossene E/A-Busteilnehmer (7) und eine Standardsteuerungseinrichtung (3), sowie wenigstens
  - einen Sicherheitsanalysator (8), welcher der den Datenfluß über das Bussystem mithört und zum Ausführen zumindest einer sicherheitsbezogenen Funktion ausgebildet ist, wobei die Standardsteuerungseinrichtung zumindest einen sicherheitsbezogenen Ausgang steuert und der Sicherheitsanalysator zum Überprüfen und/oder Verarbeiten von sicherheitsbezogenen Daten im Busdatenstrom eingerichtet ist (Spalte 1/Zeilen 34-64, Spalte 2/Zeilen 8-37, Spalte 3/Zeilen 14-34)

Der Sicherheitsanalysator weist eine programmierbare Logikeinrichtung auf, welche die abgehörten Daten, insbesondere die abgehörten sicherheitsbezogenen Daten verarbeitet (Spalte 3/Zeilen 19-22).

Der Sicherheitsanalysator (8) ist kein logischer Busteilnehmer des Automatisierungssystems und weist zumindest einen sicherheitsbezogenen Ausgang auf, über welchen wenigstens eine dem Sicherheitsanalysator zugeordnete Baugruppe des Automatisierungssystems, insbesondere wenigstens ein Busteilnehmer, ein- oder ausschaltbar ist (Spalte 3/Zeilen 26-34).

**INTERNATIONALER VORLÄUFIGER  
PRÜFUNGSBERICHT - BEIBLATT**

Internationales Aktenzeichen PCT/DE00/01901

Jedoch ist der Druckschrift nicht zu entnehmen, daß der Sicherheitsanalysator eine Einrichtung zum Manipulieren des auf dem Bus übertragenen Datenstroms aufweist.

D2 offenbart ein Automatisierungssystem, daß jedoch mit zwei unabhängigen Bussystemen ausgestattet ist.

D3 beschreibt ein dezentrales I/O-Bussystem (INTERBUS), aus der jedoch kein Sicherheitsanalysator, wie in Anspruch 1 definiert, zu entnehmen ist.

D4 beschreibt ein Automatisierungssystem umfassend ein Bussystem, daran angeschlossene E/A Busteilnehmer und ein (darunter ausgewählten) Sicherheitsanalysator (SAM), der eine "Teilnehmerliste" der aktiven Teilnehmer führt. Der Sicherheitsanalysator weist jedoch keine Einrichtung zum Manipulieren des über den Bus übertragenen Datenstroms auf.

D5 zeigt ein Verfahren zum Betrieb eines Automatisierungssystems, wobei durch eine Standardsteuerungseinrichtung, eine Prozeßsteuerung mit der Verarbeitung von prozeßgebundenen E/A-Daten und eine sicherheitsbezogene Steuerung mit der Verarbeitung von sicherheitsbezogenen Daten durchgeführt wird und weiterhin eine Verarbeitung sicherheitsbezogener Daten auf zumindest einem Sicherheitsanalysator durchgeführt wird, wobei im Sicherheitsanalysator sicherheitsbezogene Daten verarbeitet werden (Spalte 6/Zeile 48-Spalte 9/Zeile 45).

Aus diesem Grund ist der Gegenstand des unabhängigen Anspruchs 15 nicht neu (Artikel 33(2) PCT).

Der Sicherheitsanalysator aus D5 weist jedoch keine Einrichtung zum Manipulieren des über den Bus übertragenen Datenstroms auf.

D6 und D7 zeigen weitere Überwachungsvorrichtungen, welche jedoch nicht die Merkmale des Vorrichtungsanspruchs 1 aufweisen.

Aus den vorgenannten Gründen ist der Gegenstand des Anspruchs 1 neu (Artikel 33(2) PCT) gegenüber dem in den Dokumenten D1-D7 gezeigten Stand der Technik.

**INTERNATIONALER VORLÄUFIGER  
PRÜFUNGSBERICHT - BEIBLATT**

Internationales Aktenzeichen PCT/DE00/01901

Da jedes der genannten Dokumente ein verschiedenes Konzept der sicherheitsbezogenen Steuerung aufweist, ist es für den Fachmann als nicht naheliegend anzusehen, einzelne Merkmale der unterschiedlichen Systeme in den Druckschriften zu kombinieren.

Daher sind die Merkmale des Anspruchs 1, insbesondere daß der Sicherheitsanalysator eine Einrichtung zum Manipulieren des über den Bus übertragenen Datenstroms aufweist, für den Fachmann aus den Dokumenten D1-D7 nicht in offensichtlicher Weise zu entnehmen.

Folglich beruht der Gegenstand der Ansprüche 1-14 auf erfinderischer Tätigkeit (Artikel 33(3) PCT).

Die Merkmale der Ansprüche 16-22, 24-31 sind, soweit nicht schon aus dem Stand der Technik in D2-D7 bekannt lediglich naheliegende Ausführungsformen des Verfahrens zum Betrieb eines Automatisierungssystems nach Anspruch 15, zur Lösung der gestellten Aufgabe.

Daher beruhen die Gegenstände der Ansprüche 16-22, 24-31 nicht auf erfinderischer Tätigkeit (Artikel 33(3) PCT).

Das Merkmal des Anspruchs 23, nämlich daß der Sicherheitsanalysator eine Einrichtung zum Manipulieren des über den Bus übertragenen Datenstroms aufweist ist, wie vorab bereits ausgeführt weder aus einer der Druckschriften D1-D7 bekannt noch nahegelegt.

Der Gegenstand des Anspruchs 23 erfüllt damit die Erfordernisse des Artikels 33(2), (3) PCT.

**Sektion VII**

Der unabhängige Anspruch 15 ist nicht in der korrekten zweiteiligen Form nach Regel 6.3 b) PCT abgefaßt.

Die Beschreibungseinleitung ist nicht an den in den Dokumenten D1-D7 offenbarten einschlägige Stand der Technik angepaßt.

Der relevante Stand der Technik ist nicht in der Beschreibung aufgezeigt (Regel 5.1 (ii) PCT).

**INTERNATIONALER VORLÄUFIGER  
PRÜFUNGSBERICHT - BEIBLATT**

Internationales Aktenzeichen PCT/DE00/01901

**Sektion VIII**

Da der unabhängige Verfahrensanspruch 15 nicht neu ist (Sektion V), lassen die unterschiedlichen Definitionen in den weiteren Vorrichtungsansprüchen bzw. im unabhängigen Vorrichtungsanspruch 14 Unklarheiten über den eigentlich zu schützenden Gegenstand aufkommen (Artikel 6 PCT).

Angesichts des lediglich fakultativen Hinweises ("insbesondere") in Verfahrensanspruch 15 auf die Gegenstände der Ansprüche 1-14 erscheint es auch weiterhin, als ob zwischen den Vorrichtungsansprüchen 1-14 und Verfahrensanspruch 15, in welchem nicht die Funktion eine Einrichtung im Sicherheitsanalysator zur Manipulation des auf dem Bus übertragenen Datenstroms als Verfahrensschritt definiert ist, kein technischer Zusammenhang im Sinne der Regel 13.2 PCT besteht, der in einem oder mehreren gleichen bzw. entsprechenden, besonderen technischen Merkmalen zum Ausdruck kommt.

Patentansprüche:

1. Automatisierungssystem (1), ~~zumindest~~  
5 umfassend ~~zumindest~~  
- ein Bussystem (2), ~~darin~~  
- daran angeschlossene E/A-Busteilnehmer (31-38) und  
- eine Standardsteuerungseinrichtung (4; 40, 41),  
sowie ~~wenigstens~~  
10 - ~~wenigstens~~ einen Sicherheitsanalysator  
(5, 5', 5''), welcher den Datenfluß über das  
Bussystem mithört und zum Ausführen zumindest einer  
sicherheitsbezogenen Funktion ausgebildet ist,  
dadurch gekennzeichnet, daß  
15 ~~die Standardsteuerungseinrichtung zumindest einen~~  
~~sicherheitsbezogenen Ausgang steuert und daß~~  
der Sicherheitsanalysator zum Überprüfen und ~~oder~~  
Verarbeiten von sicherheitsbezogenen Daten im  
Busdatenstrom eingerichtet ist und/oder  
20 eine Einrichtung zum Manipulieren des auf dem Bus (2)  
übertragenen Datenstroms aufweist.
2. Automatisierungssystem (1) nach Anspruch 1,  
dadurch gekennzeichnet,  
25 daß durch die Standardsteuerungseinrichtung zumindest  
ein sicherheitsbezogener Ausgang gesteuert wird.
3. Automatisierungssystem (1) nach Anspruch 1 oder 2,  
2- dadurch gekennzeichnet, daß der Sicherheitsanalysator  
30 (5, 5', 5'') eine frei programmierbare Logikeinrichtung  
aufweist, welche die abgehörten Daten, insbesondere die  
abgehörten sicherheitsbezogenen Daten verarbeitet.

4. Automatisierungssystem (1) nach einem der Ansprüche 1  
~~3-~~ bis ~~oder~~ 3 2,  
dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5, 5', 5'') kein logischer  
5 Busteilnehmer des Automatisierungssystems (1) ist und  
dieser zumindest einen sicherheitsbezogenen Ausgang (6)  
aufweist, über welchen wenigstens eine dem  
Sicherheitsanalysator zugeordnete Baugruppe des  
Automatisierungssystems, insbesondere wenigstens ein  
10 Busteilnehmer (31-38), ein- oder ausschaltbar ist.
5. Automatisierungssystem (1) nach Anspruch 4 3,  
~~4-~~ dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5, 5', 5'') zur Abschaltung  
15 einer Sicherheitsinsel, eines Busstichs (8) und/oder der  
Gesamtanlage eingerichtet ist.
6. Automatisierungssystem (1) nach einem der Ansprüche 1  
~~5-~~ bis 5 4,  
20 dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5') zumindest einen  
sicherheitsbezogenen Eingang (10) aufweist, über welchen  
der Sicherheitsanalysator mit einer sicherheitsbezogenen  
Einrichtung (11) des Automatisierungssystem zur  
25 Erfassung von sicherheitsbezogenen Daten verbunden ist.
7. Automatisierungssystem (1) nach einem der Ansprüche 1  
~~6-~~ bis 6 5, dadurch gekennzeichnet, daß  
das Bussystem (2) über eine Anschaltbaugruppe (41) mit  
30 einem Host (40) verbunden ist,  
wobei die prozeßbezogene Steuerung im Host und die  
sicherheitsbezogene Steuerung in der Anschaltbaugruppe  
angeordnet ist.

8. Automatisierungssystem (1) nach einem der Ansprüche 1  
~~7-~~ bis 7 ~~6~~, dadurch gekennzeichnet, daß  
der Bus (2) ein serieller Bus ist und zumindest ein  
5 Sicherheitsanalysator (5, 5') im Fernbus-Abschnitt des  
Automatisierungssystems angeordnet ist.
9. Automatisierungssystem (1) nach Anspruch 8 ~~7~~,  
~~8-~~ dadurch gekennzeichnet, daß  
10 ein Sicherheitsanalysator (5) direkt nach dem Host (40)  
oder der Anschaltbaugruppe (41) angeordnet ist.
10. Automatisierungssystem (1) nach einem der Ansprüche 1  
~~9-~~ bis 9 ~~8~~, dadurch gekennzeichnet, daß  
15 ein Sicherheitsanalysator (5) in der Anschaltbaugruppe  
(41) angeordnet ist.
11. Automatisierungssystem (1) nach einem der vorstehenden  
~~10-~~ Ansprüche 1 bis 10 ~~9~~, dadurch gekennzeichnet, daß der  
20 Sicherheitsanalysator (5, 5', 5'') eine  
Speichereinrichtung zum Anlegen eines Prozeßabbildes  
umfaßt.
12. Automatisierungssystem (1) nach einem der vorstehenden  
25 ~~11-~~ Ansprüche 1 bis 11 ~~10~~,  
dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5, 5', 5'') eine Einrichtung  
zum Manipulieren des auf dem Bus (2) übertragenen  
~~Datenstroms, insbesondere der~~ Eingangs- und/oder  
30 Ausgangsdaten aufweist. ~~7~~



13. Automatisierungssystem (1) nach Anspruch 12 ~~11~~,  
~~12~~ dadurch gekennzeichnet, daß  
die Einrichtung im Sicherheitsanalysator (5, 5', 5'')  
Eingangs- und/oder Ausgangsdaten überschreibt und/oder  
5 Daten in den Datenstrom einfügt.
14. Automatisierungssystem (1) nach einem der vorstehenden  
~~13~~ Ansprüche 1 bis 13 ~~12~~,  
dadurch gekennzeichnet, daß  
10 zumindest ein Sicherheitsanalysator (5, 5', 5'')  
redundant aufgebaut ist.
15. Verfahren zum Betrieb eines ~~14~~ Automatisierungssystems,  
~~14~~ insbesondere eines Automatisierungssystems (1) nach  
15 einem der Ansprüche 1 bis 14 ~~13~~,  
dadurch gekennzeichnet, daß durch ~~die~~ eine  
Standardsteuerungseinrichtung (4; 40, 41), ~~die~~ eine  
Prozeßsteuerung mit der Verarbeitung von  
prozeßgebundenen E/A-Daten und eine  
20 sicherheitsbezogene Steuerung mit der Verarbeitung von  
sicherheitsbezogenen Daten durchgeführt wird und  
weiterhin eine Verarbeitung sicherheitsbezogener Daten  
auf zumindest einem Sicherheitsanalysator (5, 5', 5'')  
durchgeführt wird, wobei im Sicherheitsanalysator  
25 sicherheitsbezogene Daten, insbesondere  
sicherheitsbezogene Verknüpfungsdaten im Busdatenstrom  
verarbeitet werden.
16. Verfahren nach Anspruch 15,  
30 dadurch gekennzeichnet, daß  
die Standardsteuerungseinrichtung zumindest einen  
sicherheitsbezogenen Ausgang steuert.

17. Verfahren nach Anspruch 15 ~~14~~ oder 16,  
~~15~~ dadurch gekennzeichnet, daß  
in einem Sicherheitsanalysator (5, 5', 5'') ein  
Vergleich der über den Bus übertragenen  
sicherheitsbezogenen Verknüpfungsdaten der  
Standardsteuerungseinrichtung (4, 41) und/oder zumindest  
eines weiteren Sicherheitsanalysators (5, 5', 5'') mit  
den entsprechenden Verknüpfungsdaten des ersten  
Sicherheitsanalysators durchgeführt wird.
18. Verfahren nach einem der Ansprüche 15 ~~14~~ bis ~~oder~~ 17 ~~15~~,  
~~16~~ dadurch gekennzeichnet, daß  
die durch die Standardsteuerung (4, 41) erzeugten und  
als Ausgangsdaten über den Bus gesendeten  
Verknüpfungsdaten in zumindest einem  
Sicherheitsanalysator (5, 5', 5'') durch Nachbilden der  
sicherheitsbezogenen Verknüpfungen der  
Standardsteuerung (4, 41) überprüft werden.
19. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 18 ~~16~~,  
~~17~~ dadurch gekennzeichnet, daß  
im Ansprechen auf die Überprüfung oder den Vergleich  
durch den Sicherheitsanalysator (5, 5', 5'')  
sicherheitsbezogene Funktionen ausgeführt werden.
20. Verfahren nach einem der Ansprüche 15 bis 19,  
dadurch gekennzeichnet, daß  
das Ausführen einer sicherheitsbezogenen Funktionen  
über einen sicherheitsbezogenen Ausgang (6) des  
Sicherheitsanalysators (5, 5', 5'') erfolgt.

21. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 20 ~~17~~,  
~~18~~ dadurch gekennzeichnet, daß  
im Ansprechen auf die über den sicherheitsbezogenen  
Eingang (10) des Sicherheitsanalysators (5') erfaßten  
sicherheitsbezogenen Daten der Sicherheitsanalysator  
sicherheitsbezogene Funktionen ausführt.
22. Verfahren nach Anspruch 21 ~~18~~,  
~~19~~ dadurch gekennzeichnet, daß  
das Ausführen einer sicherheitsbezogenen Funktion das  
Ein- oder Ausschalten zumindest einer Baugruppe des  
Automatisierungsbussystems, insbesondere eines  
Busteilnehmers (32-38) umfaßt.
23. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 22 ~~19~~,  
~~20~~ dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5', 5'') mittels einer  
Einrichtung zum Manipulieren des Datenstroms auf dem Bus.  
(2) zumindest ein Datum des Datenstroms überschreibt,  
löscht und/oder zumindest ein Datum in den Bus-  
Datenstrom einfügt.
24. Verfahren nach der Anspruch 23 ~~20~~,  
~~21~~ dadurch gekennzeichnet, daß  
der Sicherheitsanalysator (5, 5', 5'') den abgehörten  
Datenstrom zumindest teilweise abspeichert und  
Eingangsdaten des Bus-Datenstroms in Ausgangsdaten des  
Bus-Datenstroms, und umgekehrt, umkopiert.

25. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 24 ~~21~~,  
~~22~~ dadurch gekennzeichnet, daß  
sicherheitsbezogenen Daten in einem  
Sicherheitsprotokoll über den Bus (2) übertragen  
werden.
- 5
26. Verfahren nach Anspruch 25 ~~22~~,  
~~23~~ dadurch gekennzeichnet, daß  
das Sicherheitsprotokoll zusätzlich zum Sicherheitsdatum  
das negierte Sicherheitsdatum, eine laufende Nummer,  
eine Adresse und/oder eine Datensicherungsinformation  
(CRC) umfaßt.
- 10
27. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 26 ~~23~~,  
15 ~~24~~ dadurch gekennzeichnet, daß  
der Bus ein nach dem Master-Slave-Prinzip arbeitendes  
System ist, wobei Daten zwischen zumindest zwei Slaves,  
insbesondere zwischen einzelnen Busteilnehmern (31-38),  
mittels einer Daten-Verbindung über wenigstens einen  
Sicherheitsanalysator (5, 5', 5'') übertragen werden,  
20 wobei der Sicherheitsanalysator Daten im Busdatenstrom  
umkopiert.
28. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 27 ~~23~~,  
25 ~~25~~ dadurch gekennzeichnet, daß  
der Bus ein nach dem Master-Slave-Prinzip arbeitendes  
System ist, wobei Daten zwischen zumindest zwei Slaves,  
insbesondere zwischen einzelnen Busteilnehmern (31-38),  
mittels einer Daten-Verbindung über die Steuerung oder  
den Master übertragen werden, wobei die Steuerung bzw.  
30 der Master Daten im Busdatenstrom umkopiert.

29. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 28 ~~25~~,  
~~26~~ dadurch gekennzeichnet, daß  
mittels eines Sicherheitsanalysators (5, 5', 5'')  
5 Qualitätsdaten erzeugt und/oder eine Aufbereitung der  
gelesenen Daten zur weiteren Verarbeitung durchgeführt  
werden.
30. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 29 ~~26~~,  
10 ~~27~~ dadurch gekennzeichnet, daß  
die in einem Sicherheitsanalysator (5') ablaufenden  
sicherheitsbezogenen Verknüpfungen zumindest teilweise  
redundant in wenigstens einem weiteren  
Sicherheitsanalysator (5'') durchgeführt und durch beide  
15 Sicherheitsanalysatoren zumindest teilweise die  
gleichen Sicherheitsfunktionen ausgeführt werden.
31. Verfahren nach einem der Ansprüche 15 ~~14~~ bis 30 ~~27~~,  
~~28~~ dadurch gekennzeichnet, daß  
20 ein Sicherheitsanalysator zumindest teilweise auch eine  
Prozeßdatenverarbeitung durchführt.

Claims

1. An automation system (1), at least comprising  
- a bus system (2),  
5 - I/O bus subscribers (31 - 38) connected to it and  
a standard control device (4; 40, 41), as well as at least  
- one safety analyzer (5, 5', 5'')  
which monitors the data flow via the bus system and  
is designed to carry out at least one safety-related  
10 function,  
characterized in that  
the standard control device controls at least one  
safety-related output, and in that the safety analyzer is  
set up for checking and/or processing safety-related data in  
15 the bus datastream.
2. The automation system (1) as claimed in claim 1,  
characterized in that  
the safety analyzer (5, 5', 5'') has a freely  
20 programmable logic device, which processes the monitored  
data, in particular the monitored safety-related data.
3. The automation system (1) as claimed in claim 1 or  
2,  
25 characterized in that  
the safety analyzer (5, 5', 5'') is not a logic bus  
subscriber in the automation system (1) and has at least one  
safety-related output (6) via which at least one assembly,  
which is associated with the safety analyzer, of the  
30 automation System, in particular at least one bus subscriber  
(31 - 38), can be switched on or off.

4. The automation system (1) as claimed in claim 3,  
characterized in that  
the safety analyzer (5, 5', 5'') is set up for  
5 switching off a safety island, a bus spur (8) and/or the  
entire system.

5. The automation system as claimed in one of claims 1  
to 4,

10 characterized in that  
the safety analyzer (5') has at least one safety-  
related input (10), via which the safety analyzer is  
connected to a safety-related device (11) in the automation  
system for detecting safety-related data.

15 6. The automation system (1) as claimed in one of  
claims 1 to 5,

characterized in that  
the bus system (2) is connected via an interface  
20 assembly (41) to a host (40), with the process-related  
control being arranged in the host, and the safety-related  
control being arranged in the interface assembly.

25 7. The automation system (1) as claimed in one of  
claims 1 to 6,

characterized in that  
the bus (2) is a serial bus, and at least one  
safety analyzer (5, 5') is arranged in the long-distance bus  
section of the automation system.

30 8. The automation system (1) as claimed in claim 7,

characterized in that  
a safety analyzer (5) is arranged directly after  
the host (40) or after the interface assembly (41).

5 9. The automation system (1) as claimed in one of  
claims 1 to 8,  
characterized in that  
a safety analyzer (5) is arranged in the interface  
assembly (41).

10 10. The automation system (1) as claimed in one of the  
preceding claims 1 to 9,  
characterized in that  
the safety analyzer (5, 5', 5'') comprises a memory  
15 device for storing a process map.

11. The automation system (1) as claimed in one of the  
preceding claims 1 to 10,  
characterized in that  
20 the safety analyzer (5, 5', 5'') has a device for  
manipulating the datastream transmitted on the bus (2), in  
particular the input and/or output data.

12. The automation system (1) as claimed in claim 11,  
25 characterized in that  
the device overwrites input and/or output data,  
and/or inserts data into the datastream.

13. The automation system (1) as claimed in one of the  
30 preceding claims 1 to 12,  
characterized in that



at least one safety analyzer (5, 5', 5'') is of redundant design.

14. A method for operating an automation system, in particular an automation system (1) as claimed in one of claims 1 to 13,

characterized in that

the standard control device (4; 40, 41) carries out the process control with the processing of process-linked I/O data and safety-related control with the processing of safety-related data, and, furthermore, processing of safety-related data is carried out in at least one safety analyzer (5, 5', 5''), with safety-related data, in particular safety-related logic linking data in the bus datastream, being processed in the safety analyzer.

15. The method as claimed in claim 14, characterized in that

a comparison of the safety-related logic linking data, which is transmitted via the bus, for the standard control device (4, 41) and/or of at least one further safety analyzer (5, 5', 5'') with the corresponding logic linking data of the first safety analyzer, is carried out in a safety analyzer (5, 5', 5'').

16. The method as claimed in one of claims 14 or 15, characterized in that

the logic linking data, which is produced by the standard control (4, 41) and is sent as output data via the bus, is checked in at least one safety analyzer (5, 5', 5'') by modeling the safetyrelated logic links of the standard

control (4, 41).

17. The method as claimed in one of claims 14 or 16,  
characterized in that  
5 safety-related functions are carried out in  
response to the check or the comparison by the safety  
analyzer (5, 5', 5'').

18. The method as claimed in one of claims 14 to 17,  
10 characterized in that  
the safety analyzer carries out safety-related  
functions in response to the safety-related data detected  
via the safety-related input (10) of the safety analyzer  
(5').

15 19. The method as claimed in claim 18,  
characterized in that  
the process of carrying out the safety-related  
function comprises switching at least one assembly in the  
20 automation bus system, in particular a bus subscriber (32 -  
38), on or off.

20. The method as claimed in one of claims 14 to 19,  
characterized in that  
25 the safety analyzer (5', 5'') overwrites or deletes  
at least one data item in the datastream and/or inserts at  
least one data item into the bus datastream by means of a  
device for manipulating the datastream on the bus (2).

30 21. The method as claimed in claim 20,  
characterized in that

the safety analyzer (5, 5', 5'') at least partially stores the monitored datastream and copies input data in the bus datastreams to output data in the bus datastream, and vice versa.

5  
22. The method as claimed in one of claims 14 to 21, characterized in that safety-related data is transmitted via the bus (2) using a security protocol.

10  
23. The method as claimed in claim 22, characterized in that, in addition to the safety data item, the security protocol comprises the negated safety data item, a  
15 sequential number, an address and/or a data protection information (CRC).

24. The method as claimed in one of claims 14 to 23, characterized in that  
20 the bus is a system operating on the master-slave principle, with data being transmitted between at least two slaves, in particular between individual bus subscribers (31 - 38), by means of a data link via at least one safety analyzer (5, 5', 5''), with the safety analyzer copying data  
25 in the bus datastream.

25. The method as claimed in one of claims 14 to 23, characterized in that  
the bus is a system operating on the master-slave  
30 principle, with data being transmitted between at least two slaves, in particular between individual bus subscribers (31

- 38), by means of a data link via the control or the master, with the control or the master copying data in the bus datastream.

- 5    26.        The method as claimed in one of claims 14 to 25,  
                 characterized in that  
                 quality data is produced by means of a safety  
                 analyzer (5, 5', 5''), and/or the data which has been read  
                 is prepared for further processing.
- 10
27.        The method as claimed in one of Cclaims 14 to 26,  
                 characterized in that  
                 the safety.related logic links used in a safety  
                 analyzer (5') are at least partially carried out in  
15               redundant form in at least one further safety analyzer  
                 (5''), and the same safety functions are at least partially  
                 carried out by the two safety analyzers.
28.        The method as claimed in one of claims 14 to 27,  
20               characterized in that  
                 a safety analyzer also at least partially carries  
                 out process data processing.

Abstract

The invention relates to a safety-related automation system, and to a method for operating such a system.

5 In order to provide a safety-related automation bus system which needs only a low level of hardware redundancy and can be flexibly matched to the respective requirements, the automation system comprises at least one safety analyzer, which is connected by means of an interface to the bus and monitors the data flow via the bus, the analyzer being set up for carrying out safety-  
10 related functions. The automation system is distinguished in that the standard control device drives at least one safety-related output, and the safety analyzer is designed for checking and/or for processing safety-related data in the bus datastream.

## PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 99PH 1131 DEP	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE00/01901	International filing date (day/month/year) 16 June 2000 (16.06.00)	Priority date (day/month/year) 17 June 1999 (17.06.99)
International Patent Classification (IPC) or national classification and IPC G05B 19/042		
Applicant PHOENIX CONTACT GMBH & CO.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 8 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 09 January 2001 (09.01.01)	Date of completion of this report 07 September 2001 (07.09.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE00/01901

## I. Basis of the report

## 1. With regard to the elements of the international application:\*

- ☐ the international application as originally filed
- ☒ the description:  
pages \_\_\_\_\_ 1-23 \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☒ the claims:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement under Article 19  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_ 1-31 \_\_\_\_\_, filed with the letter of \_\_\_\_\_ 17 August 2001 (17.08.2001)
- ☒ the drawings:  
pages \_\_\_\_\_ 1/5-5/5 \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

## 2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

## 3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.  
PCT/DE 00/01901

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

### 1. Statement

Novelty (N)	Claims	1-14, 16-31	YES
	Claims	15	NO
Inventive step (IS)	Claims	1-14, 23	YES
	Claims	16-22, 24-31	NO
Industrial applicability (IA)	Claims	1-31	YES
	Claims		NO

### 2. Citations and explanations

The following documents were interpreted as the relevant prior art for this examination:

D1: DE-A-198 15 150 (LEUZE ELECTRONIC GMBH & CO) 22 October 1998 (1998-10-22)

D2: EP-A-0 770 942 (ELAN SCHALTELEMENTE GMBH) 2 May 1997 (1997-05-02)

D3: MOHLENBEIN H: "INTERBUS-DEZENTRALE ECHTZEIT-PERIPHERIE FUER STANDARD-SPS-SYSTEME" ELEKTRIE,CC,VEB VERLAG TECHNIK. BERLIN, Vol. 44, No. 7, 1990, pages 244-249, XP000162759 ISSN: 0013-5399

D4: US-A-4 680 753 (FULTON TEMPLE L ET AL) 14 July 1987 (1987-07-14)

D5: EP-A-0 837 394 (ELAN SCHALTELEMENTE GMBH) 22 April 1998 (1998-04-22)

D6: DE-A-195 10 470 (KLASCHKA IND ELETRONIK) 17 October 1996 (1996-10-17)

D7: EP-A-0 600 311 (SQUARE D DEUTSCHLAND) 8 June 1994 (1994-06-08)

1. Document D1 shows in Figure 1 an automation system including at least:

- a bus system (1) having attached to it
- I/O bus users (7) and a standard control apparatus (3), as well as at least
- one safety analyzer (8), which monitors the data flow over the bus system and is configured to carry out at least one safety-related function, the standard control



apparatus controlling at least one safety-related output and the safety analyzer being arranged to examine and/or process safety-related data in the bus data stream (column 1, lines 34-64; column 2, lines 8-37; column 3, lines 14-34).

The safety analyzer comprises a programmable logic device that processes the monitored data, in particular the monitored safety-related data (column 3, lines 19-22).

The safety analyzer (8) is not a logical automation system bus user and has at least one safety-related output through which at least one structural component of the automation system assigned to the safety analyzer, particularly at least one bus user, can be switched on or off (column 3, lines 26-34).

However, this document does not indicate that the safety analyzer has a device for manipulating the data flow that is transmitted to the bus.

D2 discloses an automation system, but it is provided with two independent bus systems.

D3 describes a local I/O bus system (INTERBUS), but no safety analyzer as defined in Claim 1 can be found in this document.

D4 describes an automation system comprising a bus system having attached to it I/O bus users and (selected from these) a safety analyzer (SAM), which creates a "user list" of active users. The safety analyzer does not have a device for manipulating the data flow that is transmitted to the bus, though.

D5 shows a method for operating an automated system in which, using a standard control apparatus, a process control is carried out with the processing of process-bound I/O data and a safety-related control is carried out with the processing of safety-related data, and furthermore the processing of safety-related data is carried out on at least one safety analyzer, safety-related data being processed in the safety analyzer (column 6, line 48 to column 9, line 45).

For this reason, the subject matter of independent Claim 15 is not novel (PCT Article 33(2)).

However, the safety analyzer from D5 does not have a device for manipulating the data flow that is transmitted via the bus.

D6 and D7 show further monitoring devices, but they do not have the features of device Claim 1.

For the stated reasons, the subject matter of Claim 1 is novel (PCT Article 33(2)) with respect to the prior art shown in documents D1-D7.

Since each of the cited documents has a different concept of safety-related control, it is not considered obvious for a person skilled in the art to combine the individual features of the various systems in the documents.

Thus the features of Claim 1, in particular the fact that the safety analyzer comprises a device for manipulating the data flow that is transmitted to the bus, are not indicated to a person skilled in the art in an obvious way in documents D1-D7.

Accordingly, the subject matter of Claims 1-14 involves an inventive step (PCT Article 33(3)).

The features of Claims 16-22 and 24-31, if they are not already known from the prior art in D2-D7, represent nothing more than obvious embodiments of the method for operating an automated system according to Claim 15 to solve the problem of interest.

Thus the subject matter of Claims 16-22 and 24-31 does not involve the requisite inventive step (PCT Article 33(3)).

The feature of Claim 23, namely that the safety analyzer comprises a device for manipulating the data flow that is transmitted via the bus, is, as indicated earlier, neither known from nor suggested by any of documents D1-D7.

**INTERNATIONAL PRELIMINARY EXAMINATION REPORT**

International application No.

PCT/DE 00/01901

The subject matter of Claim 23 thus meets the requirements of PCT Article 33(2) and (3).

**INTERNATIONAL PRELIMINARY EXAMINATION REPORT**

International application No.  
PCT/DE 00/01901

**VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:

Independent Claim 15 has not been drafted in the proper two-part form pursuant to PCT Rule 6.3(b).

The introductory part of the description has not been adapted to the relevant prior art disclosed in documents D1-D7.

Contrary to PCT Rule 5.1(a)(ii), the description does not cite the relevant prior art.

**VIII. Certain observations on the international application**

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Since independent Claim 15 is not novel (see Box V), the different definitions in the other device claims and in independent Claim 14 cause a lack of clarity to arise regarding the subject matter for which protection is sought (PCT Article 6).

In light of the merely optional reference ("in particular") to the subject matter of Claims 1-14 in method Claim 15, it also appears as though there is no technical relationship among one or more of the same or corresponding special technical features within the meaning of PCT Rule 13.2 between device Claims 1-14 and method Claim 15, in which the function of a device in the safety analyzer for manipulating the data flow that is transmitted on the bus is not defined as a process step.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT  
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>99PH 1131 DEP</b>	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen <b>PCT/DE 00/ 01901</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>16/06/2000</b>	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>17/06/1999</b>
Anmelder  <b>PHOENIX CONTACT GMBH &amp; CO. et al.</b>		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

☐ wie vom Anmelder vorgeschlagen

☐ keine der Abb.

☒ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES  
IPK 7 G05B19/042

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
IPK 7 G05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

WPI Data, EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 198 15 150 A (LEUZE ELECTRONIC GMBH & CO) 22. Oktober 1998 (1998-10-22) das ganze Dokument	1, 5, 11, 13
Y		2-4, 6-10, 12, 14-20, 24, 25, 27, 28
X	EP 0 770 942 A (ELAN SCHALTELEMENTE GMBH) 2. Mai 1997 (1997-05-02) Zusammenfassung Spalte 6, Zeile 7 -Spalte 8, Zeile 30 Anspruch 6 Abbildung 1	1
Y		3, 4



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

\*A\* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

\*E\* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

\*L\* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

\*O\* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

\*P\* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

\*T\* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

\*X\* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

\*Y\* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

\*Z\* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

13. Dezember 2000

Absendedatum des internationalen Recherchenberichts

20/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Hurtado-Albir, J

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	MOHLENBEIN H: "INTERBUS-DEZENTRALE ECHTZEIT-PERIPHERIE FUER STANDARD-SPS-SYSTEME" ELEKTRIE,DD,VEB VERLAG TECHNIK. BERLIN, Bd. 44, Nr. 7, 1990, Seiten 244-249, XP000162759 ISSN: 0013-5399 das ganze Dokument	2,6-10
A	---	1,14, 20-23
Y	US 4 680 753 A (FULTON TEMPLE L ET AL) 14. Juli 1987 (1987-07-14)  Zusammenfassung	12, 14-20, 24,25, 27,28
X	--- EP 0 837 394 A (ELAN SCHALTELEMENTE GMBH) 22. April 1998 (1998-04-22) Zusammenfassung Spalte 6, Zeile 43 -Spalte 11, Zeile 56 Abbildungen	1
A	---	2,5-28
A	DE 195 10 470 A (KLASCHKA IND ELEKTRONIK) 17. Oktober 1996 (1996-10-17) Zusammenfassung Spalte 2, Zeile 24 -Spalte 3, Zeile 15	1-28
A	--- EP 0 600 311 A (SQUARE D DEUTSCHLAND) 8. Juni 1994 (1994-06-08) das ganze Dokument -----	1-28



# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

DE 00/01901

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
DE 19815150	A	22-10-1998	NONE		
EP 0770942	A	02-05-1997	DE 19540069	A	30-04-1997
US 4680753	A	14-07-1987	DE 3689052	D	28-10-1993
			DE 3689052	T	13-01-1994
			EP 0200365	A	05-11-1986
			JP 1894678	C	26-12-1994
			JP 6024371	B	30-03-1994
			JP 61257039	A	14-11-1986
EP 0837394	A	22-04-1998	DE 19643092	A	30-04-1998
			JP 10228426	A	25-08-1998
DE 19510470	A	17-10-1996	NONE		
EP 0600311	A	08-06-1994	DE 4240071	A	01-06-1994
			DE 59307203	D	02-10-1997

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**